

Sécurité dans les télécommunications et les technologies de l'information

Aperçu des problèmes
et présentation des
Recommandations UIT-T
existantes sur la sécurité
dans les télécommunications

UIT-T

UIT-T

Secteur de la
normalisation des
télécommunications de l'UIT

2 0 0 9



Union
internationale des
télécommunications

UIT-T – Bureau de la normalisation des télécommunications (TSB)
Place des Nations – CH-1211 Genève 20 – Suisse
E-mail: tsbmail@itu.int Web: www.itu.int/ITU-T

Sécurité dans les télécommunications et les technologies de l'information

*Aperçu des problèmes et présentation des
Recommandations UIT-T existantes sur
la sécurité dans les télécommunications*

Septembre 2009

© UIT 2010

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, par quelque procédé que ce soit, sans l'accord écrit préalable de l'UIT.

Préface

Malcolm Johnson

Directeur

Bureau de la normalisation des télécommunications de l'UIT



Jusqu'à encore récemment, la sécurité dans les télécommunications et les technologies de l'information concernait principalement des domaines spécialisés tels que les applications bancaires, aérospatiales et militaires. Toutefois, avec la croissance rapide et généralisée de l'utilisation des communications de données, et notamment de l'Internet, la sécurité est devenue l'affaire de presque tous.

L'ampleur prise par la sécurité des technologies de l'information et de la communication (TIC) peut être attribuée en partie à des incidents qui ont défrayé la chronique tels que des virus, des vers, des piratages et des menaces d'atteinte à la vie privée. Mais la réalité est que les ordinateurs et les réseaux font désormais tellement partie de la vie quotidienne, qu'il est maintenant impératif de mettre en place des mesures de sécurité efficaces afin de protéger les systèmes informatiques et de télécommunications des pouvoirs publics, des entreprises, des sociétés de commerce, des infrastructures critiques et des particuliers. Par ailleurs, de plus en plus de pays disposent maintenant d'une législation de protection des données qui exige le respect de normes reconnues de confidentialité et d'intégrité des données.

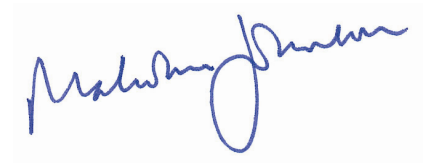
Il est désormais largement admis que la sécurité doit être intégrée aux systèmes et non pas mise en œuvre après coup et que, pour être vraiment efficace, elle doit absolument être prise en compte à toutes les étapes du cycle de vie des systèmes, depuis leur définition et leur conception jusqu'à leur mise hors service, en passant par leur implémentation et leur déploiement. Faute de prendre en compte correctement la sécurité durant la phase de conception d'un projet et durant le développement des systèmes, il peut en résulter des vulnérabilités au niveau de l'implémentation. Les comités de normalisation ont un rôle essentiel à jouer dans la protection des systèmes informatiques et de télécommunications en se tenant au courant des problèmes de sécurité, en faisant en sorte que les considérations de sécurité constituent une partie fondamentale des spécifications et en fournissant des normes techniques et des indications aux personnes chargées de l'implémentation et aux utilisateurs afin de les aider à rendre les systèmes et services de communication suffisamment robustes pour pouvoir résister aux cyberattaques.

L'UIT-T participe activement aux travaux sur la sécurité dans les télécommunications et les technologies de l'information depuis de nombreuses années. Toutefois, l'augmentation de l'utilisation des réseaux s'est traduite par une augmentation considérable de la charge de travail afin de répondre aux demandes de nos membres qui ont besoin de normes pour les aider à faire face aux menaces qui apparaissent ou qui évoluent. Ce manuel donne un aperçu de certains éléments essentiels de ces travaux et présente les nombreuses ressources mises par l'UIT-T à la disposition de tous les utilisateurs pour les aider à faire face aux problèmes qu'ils rencontrent concernant la sécurité dans les réseaux.

La normalisation est essentielle pour construire une culture mondiale de la cybersécurité. Nous pouvons venir à bout des cybermenaces et nous en viendrons à bout. Pour cela, nous tirerons parti des travaux réalisés par des milliers de personnes dévouées, issues d'administrations publiques, du secteur privé et du monde universitaire, qui, rassemblées dans des organisations comme l'UIT, élaborent des normes sur la sécurité et des lignes directrices relatives aux bonnes pratiques. Ces travaux ne sont ni fascinants, ni très en vue, mais ils n'en sont pas moins essentiels pour protéger notre avenir numérique. J'exprime toute ma gratitude aux ingénieurs du Bureau de la normalisation des télécommunications de l'UIT qui, conjointement avec des

experts provenant d'Etats Membres de l'UIT, ont travaillé et continuent de travailler inlassablement pour élaborer ces normes et lignes directrices.

Ce manuel est destiné à guider les cadres supérieurs et les dirigeants qui ont des responsabilités dans le domaine de la sécurité des informations et des télécommunications ou qui s'intéressent à ce domaine, ainsi que les techniciens, les régulateurs et toute autre personne qui souhaitent mieux comprendre les questions de sécurité des TIC et les Recommandations UIT-T correspondantes qui portent sur ces questions. Je suis certain que ce manuel sera utile à ceux qui s'intéressent aux questions de sécurité des TIC et j'invite les lecteurs à me communiquer leurs réactions en vue des éditions futures.



Malcolm Johnson

Directeur

Bureau de la normalisation des télécommunications, UIT

Table des matières

	<i>Page</i>
Préface	i
Remerciements	vii
Résumé	ix
Introduction à la 4 ^e édition	xi
1 Introduction	3
1.1 Objet et portée du présent manuel	3
1.2 Comment utiliser le présent manuel	3
2 Aperçu des activités de l'UIT-T dans le domaine de la sécurité	7
2.1 Introduction	7
2.2 Documents de référence ou de vulgarisation	7
2.3 Aperçu des principaux sujets sur la sécurité et des Recommandations associées	7
3 Spécifications de sécurité	11
3.1 Introduction	11
3.2 Menaces, risques et vulnérabilités	11
3.3 Objectifs généraux de sécurité pour les réseaux des TIC	13
3.4 Raison d'être des normes sur la sécurité	14
3.5 Evolution des normes de l'UIT-T sur la sécurité	14
3.6 Spécifications de sécurité du personnel et de sécurité physique	16
4 Architectures de sécurité	19
4.1 Architecture de sécurité pour les systèmes ouverts et normes associées	19
4.2 Services de sécurité	20
4.3 Architecture de sécurité pour les systèmes assurant des communications de bout en bout	21
4.3.1 Eléments de l'architecture UIT-T X.805	21
4.3.2 Disponibilité du réseau et de ses composants	24
4.4 Guide de mise en œuvre	24
4.5 Architectures propres à certaines applications	25
4.5.1 Communications entre homologues	25
4.5.2 Architecture de sécurité des messages dans l'environnement des services web mobiles	27
4.6 Autres architectures et modèles de sécurité de réseau	28
5 Aspects de gestion de la sécurité	31

	<i>Page</i>
5.1	Gestion de la sécurité des informations 31
5.2	Gestion des risques 32
5.3	Prise en charge des incidents 33
6	L'annuaire, authentification et gestion d'identité..... 39
6.1	Protection des informations de l'annuaire 39
6.1.1	Objectifs de protection de l'annuaire 39
6.1.2	Authentification des utilisateurs de l'annuaire..... 40
6.1.3	Contrôle d'accès à l'annuaire..... 40
6.1.4	Protection de la confidentialité 40
6.2	Authentification forte: mécanismes de sécurité à clé publique..... 41
6.2.1	Cryptographie à clé secrète et cryptographie à clé publique..... 42
6.2.2	Certificats de clé publique 44
6.2.3	Infrastructures de clé publique..... 45
6.2.4	Infrastructure de gestion de privilège 45
6.3	Lignes directrices relatives à l'authentification 47
6.3.1	Protocole d'authentification sûre fondée sur un mot de passe avec échange de clés 47
6.3.2	Protocole d'authentification extensible..... 48
6.4	Gestion d'identité..... 49
6.4.1	Aperçu de la gestion d'identité 49
6.4.2	Travaux de l'UIT-T sur la gestion d'identité 50
6.5	Télébiométrie 50
6.5.1	Authentification télébiométrique 51
6.5.2	Génération et protection des clés numériques télébiométriques 51
6.5.3	Aspects de sécurité et de sûreté de la télébiométrie..... 52
6.5.4	Télébiométrie relative à la physiologie humaine 52
6.5.5	Autres éléments définis dans les normes sur la télébiométrie..... 52
7	Sécurisation de l'infrastructure des réseaux..... 57
7.1	Le réseau de gestion des télécommunications 57
7.2	Architecture de gestion de réseau 57
7.3	Sécurisation des éléments d'infrastructure d'un réseau..... 59
7.4	Sécurisation des activités de surveillance et de contrôle 60
7.5	Sécurisation des applications fondées sur le réseau..... 62
7.6	Services communs de gestion de la sécurité..... 62
7.6.1	Fonction de signalisation des alarmes de sécurité 63
7.6.2	Fonction de piste de vérification de sécurité..... 63

	<i>Page</i>
7.6.3	Contrôle d'accès pour les entités gérées 63
7.6.4	Services de sécurité fondés sur l'architecture CORBA 64
8	Approches particulières relatives à la sécurité des réseaux 67
8.1	Sécurité des réseaux de prochaine génération (NGN) 67
8.1.1	Objectifs et spécifications de sécurité des NGN 67
8.2	Sécurité des communications mobiles 69
8.2.1	Communications mobiles sécurisées de données de bout en bout 70
8.3	Sécurité des réseaux domestiques 75
8.3.1	Cadre de sécurité pour les réseaux domestiques 75
8.3.2	Certification et authentification de dispositif dans les réseaux domestiques 76
8.3.3	Authentification des utilisateurs humains pour les services de réseau domestique . 77
8.4	IPCablecom 78
8.4.1	Architecture IPCablecom 78
8.4.2	Spécifications de sécurité pour IPCablecom 79
8.4.3	Services et mécanismes de sécurité dans IPCablecom 80
8.5	IPCablecom2 80
8.5.1	Architecture IPCablecom2 80
8.5.2	Spécifications de sécurité pour IPCablecom2 80
8.5.3	Services et mécanismes de sécurité dans IPCablecom2 81
8.6	Sécurité des réseaux de capteurs ubiquitaires 82
9	Sécurité des applications 87
9.1	Téléphonie IP (VoIP) et multimédia 87
9.1.1	Problèmes de sécurité dans le domaine du multimédia et de la téléphonie IP 88
9.1.2	Aperçu des Recommandations de la sous-série H.235.x 90
9.1.3	Traducteurs d'adresse de réseau et pare-feu 92
9.2	TVIP 94
9.2.1	Mécanismes de protection de contenu de TVIP 95
9.2.2	Mécanismes de protection de service de TVIP 96
9.2.3	Protection des informations d'abonné 96
9.3	Transmission de télécopie sécurisée 96
9.4	Services web 97
9.4.1	Langage de balisage d'assertion de sécurité 98
9.4.2	Langage de balisage extensible de contrôle d'accès 99
9.5	Services par étiquette 99
10	Lutte contre les menaces courantes dans les réseaux 105

	<i>Page</i>
10.1	Lutte contre le spam..... 105
10.1.1	Stratégies techniques de lutte contre le spam..... 105
10.1.2	Spam par courrier électronique..... 106
10.1.3	Spam multimédia IP..... 107
10.1.4	Spam du service de messages courts (SMS)..... 108
10.2	Codes malveillants, logiciels espions et logiciels trompeurs..... 108
10.3	Notification et diffusion de mises à jour logicielles..... 108
11	L'avenir de la normalisation de la sécurité des TIC..... 113
12	Sources d'informations complémentaires..... 117
12.1	Aperçu des travaux de la CE 17..... 117
12.2	Recueil sur la sécurité..... 117
12.3	Feuille de route sur les normes de sécurité..... 117
12.4	Lignes directrices pour la mise en œuvre de la sécurité..... 118
12.5	Informations complémentaires sur l'annuaire, l'authentification et la gestion d'identité..... 118
Annexe A	– Définitions relatives à la sécurité..... 121
Annexe B	– Acronymes et abréviations utilisés dans le présent manuel..... 135
Annexe C	– Présentation succincte des Commissions d'études de l'UIT-T menant des activités dans le domaine de la sécurité..... 141
Annexe D	– Recommandations sur la sécurité mentionnées dans le présent manuel..... 145

Remerciements

De nombreuses personnes ont participé à la préparation de ce manuel, en contribuant à l'élaboration de Recommandations UIT-T pertinentes ou en participant à des réunions des Commissions d'études de l'UIT-T, à des ateliers ou à des séminaires. Les remerciements vont aux Rapporteurs, aux éditeurs et aux coordonnateurs sur la sécurité des Commissions d'études de l'UIT, aux conseillers du TSB de l'UIT impliqués dans les études sur la sécurité et en particulier à Herb Bertine, l'ancien Président de la Commission d'études directrice de l'UIT-T pour les travaux sur la sécurité des télécommunications et à Mike Harrop, l'ancien Rapporteur pour le projet relatif à la sécurité.

Résumé

Ce manuel a pour objet de présenter de façon générale les travaux de l'UIT-T sur la sécurité. Il s'adresse à ceux qui ont des responsabilités en ce qui concerne la sécurité des informations et des communications et les normes associées ou qui s'intéressent à ce domaine, ainsi qu'à ceux qui cherchent simplement à mieux comprendre les questions de sécurité des TIC et les Recommandations UIT-T correspondantes.

Le texte commence par un aperçu des activités de l'UIT-T sur la sécurité, avec des liens vers certaines ressources essentielles de l'UIT-T sur la sécurité et des informations de vulgarisation. Cette partie introductive du manuel contient en outre un tableau récapitulatif qui indique comment le manuel peut être utilisé par les différentes catégories de lecteurs.

Vient ensuite un chapitre qui présente les spécifications de base pour la protection des applications des TIC, des services et des informations, qui explicite les menaces et les vulnérabilités sur lesquelles reposent les spécifications, qui examine le rôle des normes dans le respect des spécifications et qui décrit certains aspects nécessaires pour protéger les diverses parties impliquées dans l'utilisation et dans l'exploitation de fonctionnalités des TIC. On explique en outre la raison d'être des normes sur la sécurité des TIC et on présente l'évolution des travaux de l'UIT-T dans ce domaine.

Les architectures de sécurité génériques pour les systèmes ouverts et les communications de bout en bout sont ensuite présentées ainsi que les architectures propres à certaines applications. Elles établissent chacune un cadre à l'intérieur duquel les multiples facettes de la sécurité peuvent être appliquées de manière cohérente. Dans ces architectures, sont normalisés les concepts de base pour les services et les mécanismes de sécurité ainsi que les termes et concepts de base relatifs à la sécurité des TIC. Les principes généraux énoncés dans le cadre de ces architectures constituent le fondement de nombreuses autres normes sur les services, mécanismes et protocoles de sécurité. Ce chapitre donne en outre un lien vers les lignes directrices relatives à la sécurité des activités critiques associées au cycle de vie de la sécurité des réseaux.

Le chapitre suivant porte sur certains aspects de gestion de la sécurité et plus particulièrement sur la gestion de la sécurité des informations, la gestion des risques ainsi que l'intervention en cas d'incidents et la prise en charge desdits incidents.

L'annuaire et son rôle d'appui pour les services de sécurité, ainsi que les aspects associés d'authentification et de gestion d'identité sont ensuite examinés. Des aspects comme les infrastructures de clé publique, la télébiométrie (à savoir l'identification et l'authentification des personnes au moyen de dispositifs biométriques dans les environnements de télécommunication) et le respect de la vie privée sont présentés dans ce chapitre, qui porte également sur l'importance que revêt la protection de la base de données d'annuaire.

Le chapitre suivant, qui porte sur la sécurisation de l'infrastructure des réseaux, aborde des aspects liés à la gestion des réseaux et aux services communs de gestion de la sécurité.

Vient ensuite une description d'approches particulières relatives à la sécurité des réseaux. Dans ce chapitre, on commence par s'intéresser aux spécifications de sécurité pour les réseaux de prochaine génération, puis aux réseaux de communications mobiles qui passent d'une mobilité fondée sur une seule technologie (comme CDMA ou GSM) à une mobilité à travers des plateformes hétérogènes utilisant le protocole Internet. On examine ensuite les spécifications de sécurité pour les réseaux domestiques et la télévision par câble et enfin les problèmes de sécurité dans les réseaux de capteurs ubiquitaires.

Aujourd'hui, les développeurs d'application font davantage attention à la nécessité d'intégrer la sécurité dans leurs produits, plutôt que d'essayer de mettre en œuvre la sécurité après coup au stade de la production. Mais les applications restent exposées à des risques liés à l'évolution de l'environnement des menaces et aux

vulnérabilités intrinsèques. Dans le chapitre portant sur la sécurité des applications, on passe en revue un certain nombre d'applications des TIC, dont la téléphonie IP, la TVIP et la transmission de télécopie sécurisée, en mettant tout particulièrement l'accent sur les fonctionnalités de sécurité qui sont définies dans les Recommandations UIT-T.

Dans le chapitre suivant, qui porte sur la lutte contre certaines menaces courantes dans les réseaux (spam, code malveillant, logiciel espion, etc.), on souligne l'importance de notifier et diffuser rapidement les mises à jour et la nécessité de prendre en charge les incidents de sécurité de façon organisée et cohérente.

En conclusion, un bref chapitre donne les futures orientations probables concernant la normalisation de la sécurité des TIC, suivie par un chapitre qui indique des sources d'informations complémentaires.

On trouvera en Annexes des définitions, les acronymes utilisés dans le présent manuel, une présentation succincte des Commissions d'études menant des activités dans le domaine de la sécurité et la liste complète des Recommandations mentionnées dans le présent manuel.

Introduction à la 4^e édition

Pour cette 4^e édition du manuel, la structure et le contenu ont fait l'objet d'une révision importante. Depuis la publication de la première édition du manuel en 2003, l'UIT-T a entrepris des travaux dans un grand nombre de nouveaux domaines. De plus, de très nombreuses nouvelles Recommandations ont été achevées et publiées et les Commissions d'études ont été restructurées à la suite de l'Assemblée mondiale de normalisation des télécommunications (AMNT) de 2008. Toute tentative de rendre compte en détail de tous ces travaux aurait donné lieu à un document volumineux, complexe et difficile à utiliser. Après consultation des membres de l'UIT-T, certains principes directeurs ont été établis pour cette édition, à savoir:

- faire en sorte que la publication attire un public large et essayer d'éviter d'employer une terminologie et des termes complexes qui risquent de n'être compris que par les spécialistes des domaines considérés;
- faire en sorte que le texte complète les documents existants disponibles sous d'autres formes (par exemple les Recommandations) et éviter les redondances;
- rédiger le manuel de manière à pouvoir le publier à la fois en tant que document imprimé autonome et en tant que document électronique;
- employer dans le texte le plus possible d'hyperliens vers les Recommandations et les autres sources de données accessibles par tous et faire en sorte que les informations détaillées qui ne sont pas absolument indispensables pour répondre aux objectifs de base soient accessibles par le biais d'hyperliens; et
- faire en sorte, dans la mesure du possible, que le texte porte sur des travaux qui ont été achevés et publiés, et non sur des travaux en cours ou en projet.

Compte tenu de ces objectifs, le manuel n'a pas pour objet de rendre compte de tous les travaux de l'UIT-T en matière de sécurité, qu'ils soient achevés ou engagés. En revanche, certains aspects essentiels ont été privilégiés et des informations complémentaires sont accessibles par le biais d'hyperliens.

Le manuel est publié à la fois en format papier et sous forme électronique. Pour les lecteurs qui utilisent une version électronique du texte, des hyperliens directs sont fournis vers les Recommandations énumérées et vers les autres documents en ligne. Pour les lecteurs qui utilisent le format papier, toutes les Recommandations mentionnées sont énumérées dans l'Annexe D et sont accessibles en ligne à l'adresse suivante: www.itu.int/rec/T-REC/en

1. Introduction

1 Introduction

1.1 Objet et portée du présent manuel

Le présent manuel a été élaboré pour présenter les travaux de l'UIT-T sur la sécurité des télécommunications aux cadres supérieurs et dirigeants qui ont des responsabilités en ce qui concerne la sécurité des TIC et les normes associées ou qui s'intéressent à ce domaine. Il sera également utile à ceux qui souhaitent mieux comprendre les questions de sécurité des TIC et les Recommandations UIT-T correspondantes.

Le manuel donne un aperçu de la sécurité dans les télécommunications et les technologies de l'information, examine certains problèmes pratiques associés et indique comment les différents aspects de la sécurité des TIC sont abordés dans les travaux de normalisation de l'UIT-T. Il contient un texte didactique ainsi que des liens vers des informations plus détaillées et vers des documents de référence complémentaires. En particulier, il contient des liens directs vers les Recommandations UIT-T et vers des documents de référence ou de vulgarisation associés. Il rassemble en une même publication certaines informations relatives à la sécurité contenues dans les Recommandations UIT-T et explique les relations entre les divers aspects des travaux. Il tient compte des réalisations de l'UIT-T en matière de normalisation dans le domaine de la sécurité depuis la deuxième édition. Le manuel porte essentiellement sur des travaux déjà achevés. Les résultats des travaux en cours feront l'objet de futures éditions du manuel.

En plus de l'UIT-T, le Secrétariat général et les autres Secteurs de l'UIT mènent aussi des travaux dans le domaine de la sécurité. On peut citer par exemple les travaux sur la cybersécurité (www.itu.int/cybersecurity) et le Rapport de l'UIT-D sur les bonnes pratiques.

1.2 Comment utiliser le présent manuel

Le présent manuel a pour objet de donner un aperçu large et de haut niveau des activités de l'UIT-T relatives aux normes sur la sécurité. Pour ceux qui souhaitent obtenir des informations plus détaillées sur les Recommandations publiées et autres documents connexes, des liens directs sont fournis. Le manuel peut être utilisé de diverses manières. Le Tableau 1 indique comment les différentes catégories de lecteurs peuvent l'utiliser pour répondre à leurs besoins.

Tableau 1 – Manière dont le manuel répond aux besoins des différentes catégories de lecteurs

Organisation	Catégorie de lecteurs	Besoins	Manière dont le manuel permet de répondre aux besoins
Fournisseurs de services de télécommunication	Cadres supérieurs/ dirigeants	Large aperçu de la portée des efforts de normalisation Feuille de route de haut niveau concernant les normes applicables	Le manuel répond directement à ces besoins
	Ingénieurs conception et déploiement	Feuille de route concernant les normes applicables Détails techniques dans des domaines particuliers	Le manuel fournit une feuille de route et des liens vers des explications détaillées Les Recommandations donnent des détails techniques
Vendeurs de services de télécommunication	Cadres supérieurs/ dirigeants	Large aperçu de la portée des efforts de normalisation Feuille de route de haut niveau concernant les normes applicables	Le manuel répond directement à ces besoins
	Gestionnaires de produits	Feuille de route concernant les normes applicables	Le manuel fournit une feuille de route et des liens vers des explications détaillées
	Conception de produit	Détails techniques dans des domaines particuliers	Le manuel fournit des liens vers des explications détaillées dans des domaines particuliers Les Recommandations donnent des détails techniques
Utilisateurs finals	Techniques	Peuvent être intéressés par des détails techniques dans des domaines particuliers	Le manuel fournit des liens vers des explications détaillées dans des domaines particuliers
	Non techniques	Peuvent être intéressés par un large aperçu de la portée des efforts de normalisation	Le manuel répond directement à ces besoins
Monde universitaire	Etudiants / professeurs	Feuille de route concernant les normes applicables Détails techniques dans des domaines particuliers Être au courant des activités de normalisation nouvelles et à venir	Le manuel fournit une feuille de route et des liens vers des explications détaillées dans des domaines particuliers
Pouvoirs publics	Cadres supérieurs/ dirigeants	Large aperçu de la portée des efforts de normalisation Feuille de route de haut niveau concernant les normes applicables	Le manuel répond directement à ces besoins
	Régulateurs		
	Décideurs		
Organisations non gouvernementales	Cadres supérieurs/ dirigeants	Large aperçu de la portée des efforts de normalisation Feuille de route de haut niveau concernant les normes applicables	Le manuel répond directement à ces besoins
	Perfectionnement et renforcement des capacités	Feuille de route concernant les normes applicables Détails techniques dans des domaines particuliers	Le manuel fournit des liens vers des explications détaillées dans des domaines particuliers Les Recommandations donnent des détails techniques

2. Aperçu des activités de l'UIT-T dans le domaine de la sécurité

2 Aperçu des activités de l'UIT-T dans le domaine de la sécurité

2.1 Introduction

L'UIT-T travaille dans le domaine de la sécurité des TIC depuis plus de vingt ans, période pendant laquelle plusieurs Commissions d'études ont élaboré des Recommandations et des orientations dans un certain nombre de domaines essentiels. Les travaux de l'UIT-T sur la sécurité sont maintenant essentiellement confiés à la Commission d'études 17 (CE 17), qui a été désignée Commission d'études directrice pour la sécurité. Toutefois, il existe des aspects liés à la sécurité dans la plupart des domaines étudiés par l'UIT-T et la plupart des Commissions d'études mènent des travaux sur la sécurité en lien avec leur propre domaine de compétence.

En tant que Commission d'études directrice pour la sécurité, la CE 17 a élaboré un certain nombre de publications de référence ou de vulgarisation. Ces publications, qui comprennent le présent manuel, facilitent la coordination des travaux sur la sécurité au sein de l'UIT-T et contribuent à promouvoir les travaux auprès d'une communauté de plus en plus large et à encourager l'utilisation des Recommandations.

Le présent chapitre contient un aperçu des publications de référence ou de vulgarisation de l'UIT-T et récapitule les travaux engagés dans le domaine de la sécurité.

2.2 Documents de référence ou de vulgarisation

L'UIT-T tient à jour un certain nombre de publications et de sites web à partir desquels il est possible d'obtenir des informations plus détaillées sur les Recommandations et les travaux de l'UIT-T dans le domaine de la sécurité.

Sur le site web de la Commission d'études 17, qui est la Commission d'études directrice pour la sécurité, on trouvera une récapitulation des attributions et des activités de la CE 17 ainsi qu'une brève description des documents, y compris les documents de vulgarisation, avec des liens vers lesdits documents, des informations sur les ateliers passés, les exposés et les activités de vulgarisation, et des liens vers des orientations en matière de sécurité, y compris un exposé didactique sur l'écriture de programmes sûrs et sécurisés.

Pour plus de détails sur divers aspects des travaux sur la sécurité, on se reportera au chapitre 12, qui contient également des liens directs vers d'autres informations.

2.3 Aperçu des principaux sujets sur la sécurité et des Recommandations associées

Le Tableau 2 énumère certains sujets essentiels et les Recommandations associées examinés dans le présent manuel. Pour les lecteurs qui utilisent une version électronique du texte, des hyperliens directs sont fournis vers le texte relatif à chaque sujet et sous-sujet et vers les Recommandations énumérées. L'Annexe D contient la liste complète des Recommandations mentionnées dans le présent manuel. Des hyperliens sont inclus dans l'Annexe D, ce qui permet, à partir de la version électronique du texte, d'accéder directement aux Recommandations et de les télécharger.

Tableau 2 – Aperçu de certains sujets essentiels et de certaines Recommandations

Sujet	Sous-sujet	Exemples de Recommandations et publications associées
3. Spécifications de sécurité	3.2 Menaces, risques et vulnérabilités 3.3 Objectifs de sécurité 3.4 Raison d'être des normes sur la sécurité 3.6 Spécifications de sécurité du personnel et de sécurité physique	X.1205: Présentation générale de la cybersécurité E.408: Prescriptions de sécurité des réseaux de télécommunication X.1051: Lignes directrices pour la gestion de la sécurité des informations pour les organisations de télécommunication Technologies des installations extérieures appliquées aux réseaux publics Application des ordinateurs et des microprocesseurs à la fabrication, à l'installation et à la protection des câbles de télécommunication
4. Architectures de sécurité	4.1 Architecture de sécurité pour les systèmes ouverts 4.2 Services de sécurité 4.3 Architecture de sécurité pour les systèmes assurant des communications de bout en bout 4.3.2 Disponibilité du réseau et de ses composants 4.4 Guide de mise en œuvre 4.5 Architectures propres à certaines applications	X.800: Architecture de sécurité des systèmes ouverts X.805: Architecture de sécurité pour les systèmes assurant des communications de bout en bout X.810: Cadres de sécurité pour les systèmes ouverts: aperçu général X.Sup3: série UIT-T X.800-X.849 - Lignes directrices pour la mise en œuvre de la sécurité dans les systèmes et dans les réseaux X.1162: Architecture de sécurité et opérations dans les réseaux entre homologues X.1161: Cadre général des communications sécurisées entre homologues X.1143: Architecture de sécurité des messages dans l'environnement des services web mobiles.
5. Gestion de la sécurité	5.1 Gestion de la sécurité des informations 5.2 Gestion des risques 5.3 Prise en charge des incidents	X.1051: Lignes directrices pour la gestion de la sécurité des informations pour les organisations de télécommunication X.1055: Guide concernant la gestion des risques et les profils de risques pour les organisations de télécommunication E.409: Organisation en cas d'incident et prise en charge des incidents relatifs à la sécurité
6. L'annuaire, authentification et gestion d'identité	6.1 Protection des informations de l'annuaire 6.1.4 Protection de la confidentialité 6.2 Mécanismes de sécurité à clé publique 6.2.3 Infrastructures de clé publique 6.4 Gestion d'identité 6.5 Télébiométrie	X.500: L'annuaire: aperçu général des concepts, modèles et services X.509: L'annuaire: cadre général des certificats de clé publique et d'attribut X.1171: Menaces et protection requise pour les informations d'identification personnelle dans les applications utilisant l'identification par étiquette Y.2720: Cadre de gestion d'identité dans les NGN X.1081: Cadre général pour la spécification des aspects de sécurité et d'innocuité de la télébiométrie, X.1089: Infrastructure d'authentification télébiométrique
7. Sécurisation de l'infrastructure des réseaux	7.1 Le réseau de gestion des télécommunications 7.2 Architecture de gestion de réseau 7.4 Sécurisation des activités de surveillance et de contrôle 7.5 Sécurisation des applications fondées sur le réseau 7.6 Services communs de gestion de la sécurité 7.6.4 Services de sécurité fondés sur l'architecture CORBA	M.3010: Principes du réseau de gestion des télécommunications X.790: Fonction de gestion des dérangements pour les applications de l'UIT-T X.711: Protocole commun d'information de gestion: spécification X.736: Fonction de signalisation des alarmes de sécurité X.740: Fonction de piste de vérification de sécurité X.780: Directives concernant le RGT pour la définition d'objets gérés CORBA
8. Approches particulières relatives à la sécurité des réseaux	8.1 Sécurité des réseaux de prochaine génération (NGN) 8.2 Sécurité des communications mobiles 8.3 Sécurité des réseaux domestiques 8.4 Spécifications de sécurité pour IPCablecom 8.6 Sécurité des réseaux de capteurs ubiquitaires	Y.2001: Aperçu général des réseaux de prochaine génération Y.2701: Prescriptions de sécurité des réseaux de prochaine génération de version 1 X.1121: Cadre général des technologies de la sécurité pour les communications mobiles de données de bout en bout X.1111: Cadre général des technologies de sécurité pour les réseaux domestiques J.170: Spécification de la sécurité sur IPCablecom
9. Sécurité des applications	9.1 Téléphonie IP (VoIP) et multimédia 9.2 TVIP 9.3 Transmission de télécopie sécurisée 9.4 Services web 9.5 Services par étiquette	H.235: Cadre de sécurité pour les systèmes multimédias de la série H X.1191: Spécifications fonctionnelles et architecture concernant les aspects de sécurité de la TVIP T.36: Capacités de sécurité à utiliser avec les télécopieurs du Groupe 3 X.1141: Langage de balisage d'assertion de sécurité (SAML 2.0)
10. Lutte contre les menaces courantes dans les réseaux	10.1 Lutte contre le spam 10.2 Codes malveillants, logiciels espions et logiciels trompeurs 10.3 Notification et diffusion de mises à jour logicielles	X.1231: Stratégies techniques de lutte contre le spam X.1240: Technologies intervenant dans la lutte contre le spam par courrier électronique X.1244: Aspects généraux de la lutte contre le spam dans les applications multimédias IP X.1207: Lignes directrices à l'intention des fournisseurs de services de télécommunication pour lutter contre les risques d'installation de logiciels espions ou de tout logiciel potentiellement indésirable X.1206: Cadre indépendant du fournisseur de produits pour la notification automatique d'informations de sécurité et la diffusion automatique de mises à jour
On trouvera l'ensemble complet des Recommandations de l'UIT-T sur la sécurité à l'adresse: http://www.itu.int/ITU-T/recommendations/		

3. Spécifications de sécurité

3 Spécifications de sécurité

3.1 Introduction

Pour élaborer un cadre de sécurité, quel qu'il soit, il est très important d'avoir une idée claire des spécifications. Un tour d'horizon complet des spécifications de sécurité doit prendre en compte: les parties concernées, les actifs nécessitant une protection, les menaces vis-à-vis desquelles ces actifs doivent être protégés, les vulnérabilités associées aux actifs et le risque global encouru par les actifs compte tenu de ces menaces et vulnérabilités.

Le présent chapitre donne un aperçu des spécifications de base pour la protection des applications des TIC, des services et des informations, explicite les menaces et les vulnérabilités sur lesquelles reposent les spécifications, examine le rôle des normes dans le respect des spécifications et identifie certains aspects nécessaires pour protéger les diverses parties impliquées dans l'utilisation et dans l'exploitation de fonctionnalités des TIC.

Les spécifications de sécurité sont génériques ou dépendantes du contexte. Qui plus est, certaines spécifications sont bien établies alors que d'autres continuent à évoluer à mesure que de nouvelles applications apparaissent et que l'environnement des menaces évolue. Le présent chapitre porte essentiellement sur les spécifications génériques, les spécifications applicables à des applications ou des environnements particuliers étant examinées dans d'autres chapitres.

3.2 Menaces, risques et vulnérabilités

D'une manière générale, dans le domaine de la sécurité des TIC, les parties pouvant nécessiter une protection des actifs sont les suivantes:

- *les clients/abonnés*, qui veulent que le réseau et les services offerts soient fiables et que les services soient disponibles (notamment les services d'urgence);
- *la communauté/les autorités publiques*, qui exigent que la sécurité fasse l'objet de directives et/ou de lois, afin de garantir la disponibilité des services, une concurrence loyale et la protection de la vie privée; et
- *les opérateurs de réseau/fournisseurs de service* proprement dits, qui ont besoin de sécurité pour sauvegarder leurs intérêts opérationnels et commerciaux et pour satisfaire à leurs obligations vis-à-vis des clients et du grand public, au niveau national comme au niveau international.

Les actifs à protéger sont les suivants:

- services de communications et services informatiques;
- informations et données, notamment les logiciels et les données concernant les services de sécurité;
- personnel; et
- équipements et installations.

Une *menace de sécurité* est définie comme étant une violation potentielle de la sécurité, par exemple:

- divulgation non autorisée d'informations;
- destruction ou modification non autorisée de données, d'équipements ou d'autres ressources;
- vol, suppression ou perte d'informations ou d'autres ressources;
- interruption ou déni de services; et
- usurpation de l'identité d'une entité autorisée.

Les menaces peuvent être *accidentelles* ou *délibérées* et peuvent être *actives* ou *passives*. Une menace accidentelle est une menace sans préméditation (par exemple dysfonctionnement d'un système ou d'un logiciel ou défaillance physique). Une menace délibérée est une menace dont la mise à exécution est un acte délibéré commis par une personne. Les menaces délibérées vont de l'examen occasionnel à l'aide d'outils de surveillance faciles d'accès, à des attaques sophistiquées reposant sur une connaissance spéciale du système. Lorsqu'une menace délibérée est mise à exécution, on parle alors d'*attaque*. Une menace active est une menace résultant d'une modification de l'état ou du fonctionnement d'un système (par exemple altération de données ou destruction d'un équipement physique). Pour une menace passive, il n'y a pas de modification d'état (par exemple écoute clandestine).

Une *vulnérabilité de sécurité* est un défaut ou une faiblesse susceptible d'être exploité pour violer un système ou les informations qu'il contient. Si une vulnérabilité existe, il est alors possible qu'une menace soit mise à exécution.

Dans les Recommandations UIT-T, quatre types de vulnérabilité sont pris en considération:

- les vulnérabilités du modèle des menaces proviennent de la difficulté à prévoir les éventuelles menaces futures;
- les vulnérabilités de conception et spécification résultent d'erreurs ou d'oublis dans la conception d'un système ou d'un protocole qui le rendent intrinsèquement vulnérable;
- les vulnérabilités d'implémentation proviennent d'erreurs au cours de l'implémentation d'un système ou d'un protocole; et
- les vulnérabilités d'exploitation et de configuration proviennent d'un mauvais usage d'options dans des implémentations ou de politiques et de pratiques de déploiement déficientes (par exemple la non-utilisation du chiffrement dans un réseau sans fil).

Un *risque de sécurité* est une mesure des effets négatifs qui peuvent se produire en cas d'exploitation d'une vulnérabilité de sécurité, autrement dit si une menace est mise à exécution. Le risque ne peut jamais être éliminé mais un objectif de la sécurité est de réduire le risque à un niveau acceptable. Pour cela, il faut comprendre les menaces et les vulnérabilités applicables et appliquer des contremesures appropriées. Il s'agit généralement de services et de mécanismes de sécurité auxquels peuvent s'ajouter des mesures non techniques (sécurité physique et sécurité du personnel par exemple).

Alors que les menaces et les agents responsables de menaces changent, les vulnérabilités de sécurité existent pendant toute la durée de vie d'un système ou d'un protocole, sauf si des mesures spécifiques sont prises pour y faire face. Les protocoles normalisés étant très largement utilisés, toute vulnérabilité associée à un protocole peut avoir des conséquences très graves et concerner le monde entier. Il est donc particulièrement important de comprendre et de détecter les vulnérabilités présentes dans les protocoles et de prendre des mesures pour y faire face une fois qu'elles ont été détectées.

Les organismes de normalisation ont à la fois une certaine responsabilité et une compétence unique pour ce qui est de faire face aux vulnérabilités de sécurité susceptibles d'être présentes dans des spécifications d'architectures, de cadres, de protocoles, etc. Même avec une bonne connaissance des menaces, des risques et des vulnérabilités associés aux réseaux informatiques et aux réseaux de télécommunication, il est impossible d'obtenir une sécurité correcte si on n'applique pas systématiquement des mesures de sécurité conformément aux politiques en vigueur, lesquelles doivent être examinées et mises à jour régulièrement. Il faut aussi prévoir correctement la gestion de la sécurité et l'intervention en d'incidents, par exemple déterminer les responsabilités et les mesures à prendre concernant la prévention, la détection, l'examen et la prise en charge des incidents de sécurité.

Des services et des mécanismes de sécurité peuvent protéger les réseaux de télécommunication contre les attaques malveillantes telles que le déni de service, l'écoute clandestine, l'usurpation d'identité, l'altération des messages (modification, retard, suppression, insertion, relecture, réacheminement, déroutement ou réordonnancement de messages), la répudiation ou la falsification. Les techniques de protection comprennent la prévention et la détection des attaques et le retour à la normale après une attaque ainsi que la gestion des

informations liées à la sécurité. La protection doit comprendre des mesures visant à empêcher les interruptions de service dues à des événements naturels (tempêtes et séismes par exemple) ou à des attaques malveillantes (actes délibérés ou violents). Des dispositions doivent aussi être prises pour faciliter l'interception et la surveillance par les autorités judiciaires dûment autorisées.

La sécurité des réseaux de télécommunication nécessite également une large coopération entre les fournisseurs de service. La Recommandation UIT-T E.408, *Prescriptions de sécurité des réseaux de télécommunication*, donne un aperçu général des prescriptions de sécurité et définit un cadre qui identifie les menaces de sécurité dans les réseaux de télécommunication en général (fixes et mobiles; voix et données) et qui indique comment planifier des contre-mesures afin de limiter les risques découlant de ces menaces. La mise en application des prescriptions énoncées dans la Rec. UIT-T E.408 favorisera la coopération internationale dans les domaines ci-après concernant la sécurité des réseaux de télécommunication:

- partage et diffusion des informations;
- coordination en cas d'incident et réaction en cas de crise;
- recrutement et formation de professionnels de la sécurité;
- coordination de l'application de la loi;
- protection des infrastructures et services critiques; et
- élaboration d'une législation appropriée.

Toutefois, pour faciliter cette coopération, il est essentiel d'appliquer à l'échelle nationale les prescriptions concernant les composants nationaux du réseau.

La Recommandation UIT-T X.1205, *Présentation générale de la cybersécurité*, décrit les différentes menaces de sécurité du point de vue d'une organisation et examine les menaces dans les diverses couches d'un réseau.

3.3 Objectifs généraux de sécurité pour les réseaux des TIC

Les objectifs généraux de sécurité pour les réseaux de télécommunication sont les suivants:

- a) seuls les utilisateurs autorisés devraient pouvoir accéder aux réseaux de télécommunication et les utiliser;
- b) les utilisateurs autorisés devraient pouvoir accéder aux actifs pour lesquels ils disposent d'autorisations d'accès et opérer sur ces actifs;
- c) les réseaux de télécommunication devraient offrir le niveau de respect de la vie privée fixé par les politiques de sécurité qui leur sont applicables;
- d) tous les utilisateurs devraient être tenus responsables de leurs actions et uniquement de leurs actions dans les réseaux de télécommunication;
- e) afin d'en garantir la disponibilité, les réseaux de télécommunication devraient être protégés contre les accès et les opérations non sollicités;
- f) il devrait être possible d'extraire des informations relatives à la sécurité à partir des réseaux de télécommunication (mais seuls les utilisateurs autorisés devraient pouvoir extraire ces informations);
- g) lorsque des violations de la sécurité sont détectées, elles devraient être prises en charge de façon contrôlée conformément à un plan prédéfini de manière à minimaliser les dommages potentiels;
- h) en cas de détection d'une atteinte à la sécurité, il devrait être possible de rétablir les niveaux de sécurité normaux; et
- i) l'architecture de sécurité des réseaux de télécommunication devrait offrir une certaine souplesse afin de prendre en charge différentes politiques de sécurité et des mécanismes de sécurité ayant différents niveaux de robustesse.

Les objectifs (a) à (e) peuvent être remplis en mettant en œuvre les services de sécurité suivants:

- la confidentialité;
- l'intégrité des données, des systèmes et des programmes;
- la responsabilité, y compris l'authentification, la non-répudiation et le contrôle d'accès; et
- la disponibilité.

Le réseau de prochaine génération (NGN) est un type de réseau des TIC dont l'importance s'accroît rapidement. Les spécifications et objectifs de sécurité concernant les NGN sont examinés dans le chapitre 8.

3.4 Raison d'être des normes sur la sécurité

Différentes entités ont besoin d'un cadre de sécurité de réseau générique pour les télécommunications internationales: les clients/abonnés, la communauté/les autorités publiques et les opérateurs de réseau/fournisseurs de service. Il est préférable que les spécifications de sécurité pour les réseaux de télécommunication fassent l'objet de normes adoptées à l'échelle internationale. En effet, cette façon de procéder permet d'encourager des approches communes et de faciliter l'interconnexion et s'avère plus rentable que d'élaborer des approches individuelles pour chaque juridiction.

Dans certains cas, la mise en place et l'utilisation de services et de mécanismes de sécurité peuvent s'avérer relativement onéreuses par rapport à la valeur des actifs protégés. Il est donc important de pouvoir adapter les services et les mécanismes de sécurité aux besoins locaux. Toutefois, la possibilité d'adapter la sécurité peut aussi donner lieu à un certain nombre de combinaisons possibles de fonctions de sécurité. Par conséquent, il est souhaitable de disposer de *profils de sécurité* qui couvrent une grande variété de réseaux et services de télécommunication afin d'harmoniser les options dans les différentes mises en œuvre. La normalisation et l'utilisation de profils normalisés facilitent l'interopérabilité et la réutilisation de solutions et de produits, ce qui signifie que la sécurité peut être mise en œuvre plus rapidement et à un moindre coût.

Les solutions de sécurité normalisées présentent des avantages importants pour les fabricants et les utilisateurs des systèmes: réalisation d'économies d'échelle lors de l'élaboration des produits et interfonctionnement des composants dans les réseaux de télécommunication.

3.5 Evolution des normes de l'UIT-T sur la sécurité

Ces dernières années, les travaux menés par l'UIT-T dans le domaine de la sécurité ont considérablement évolué, comme nous le verrons dans d'autres chapitres, dans lesquelles un grand nombre de Recommandations individuelles sont examinées plus en détail. On aborde ici certains aspects essentiels de cette évolution, plus particulièrement en ce qui concerne les spécifications de sécurité.

D'une manière générale, les spécifications de sécurité des TIC sont définies sur la base des menaces qui pèsent sur le réseau et/ou le système, des vulnérabilités intrinsèques au réseau et/ou au système et des mesures qu'il faut prendre pour lutter contre les menaces et réduire les vulnérabilités. Les spécifications de protection concernent le réseau et ses composants. Les concepts fondamentaux liés à la sécurité, y compris les menaces, les vulnérabilités et les contremesures de sécurité, sont définis dans la Rec. UIT-T X.800, *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT*, qui a été publiée en 1991. La Rec. UIT-T E.408, *Prescriptions de sécurité des réseaux de télécommunication*, que nous avons déjà mentionnée et qui a été publiée en 2004, s'appuie sur les concepts et la terminologie de la Rec. UIT-T X.800. La Recommandation UIT-T E.408 a un caractère générique et n'identifie pas ou ne traite pas de spécifications correspondant à des réseaux particuliers. Aucun nouveau service de sécurité n'est envisagé. La Recommandation repose en revanche sur l'utilisation de services de sécurité existants définis dans d'autres Recommandations UIT-T et dans des normes élaborées par d'autres organismes.

La nécessité de lutter contre des menaces de cybersécurité toujours plus nombreuses et plus diverses (virus, vers, chevaux de Troie, attaques par usurpation d'identité, vol d'identité, spam et autres formes de

cyberattaque) est prise en compte dans la Recommandation UIT-T X.1205, *Présentation générale de la cybersécurité*, qui a été publiée en 2008. Cette Recommandation a pour objet d'élaborer une base de connaissances qui puisse faciliter la sécurisation des réseaux de demain. Elle traite de diverses technologies disponibles pour remédier aux menaces: routeurs, pare-feu, protection antivirus, systèmes de détection des intrusions, systèmes de protection contre les intrusions, informatique sécurisée, audit et surveillance, etc. Elle aborde les principes de protection des réseaux, par exemple la défense en profondeur et la gestion d'accès. Elle traite des stratégies et techniques de gestion des risques, y compris de l'importance de la formation et de la sensibilisation à la protection du réseau. En outre, des exemples sont fournis concernant la sécurisation de divers réseaux compte tenu des technologies présentées.

La Recommandation UIT-T X.1205 définit la cybersécurité comme étant l'ensemble des outils, politiques, concepts de sécurité, mécanismes de sécurité, lignes directrices, méthodes de gestion des risques, actions, formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour protéger le cyberenvironnement et les actifs des organisations et des utilisateurs. Ces actifs comprennent les dispositifs informatiques connectés, les utilisateurs de l'informatique, les applications/services, les systèmes de communication, les communications multimédias et la totalité des informations transmises et/ou stockées dans le cyberenvironnement. Telle qu'elle est définie dans cette Recommandation, la cybersécurité a pour objet de garantir que les propriétés de sécurité des organisations (disponibilité, intégrité et confidentialité) sont assurées et maintenues et de protéger les actifs des utilisateurs contre les risques qui pèsent sur la sécurité dans le cyberenvironnement.

Dans l'environnement actuel des entreprises, le concept de périmètre disparaît. Les frontières entre réseau interne et réseau externe sont de plus en plus minces. Les applications fonctionnent sur les réseaux sur la base de couches. La sécurité doit absolument être garantie à l'intérieur de chacune de ces couches et entre elles. Une approche de la sécurité par couches permet aux organisations de créer plusieurs niveaux de défense contre les menaces.

Des techniques de cybersécurité peuvent être utilisées pour garantir la disponibilité des systèmes, l'intégrité, l'authenticité, la confidentialité et la non-répudiation, pour garantir le respect de la vie privée des utilisateurs ainsi que pour établir la fiabilité des utilisateurs.

Les organisations doivent mettre au point un plan de sécurité détaillé adapté à chaque contexte particulier. La sécurité n'est pas "à taille unique". Elle doit être prise en considération dans le cadre d'un processus permanent de protection des systèmes, des réseaux, des applications et des ressources. Elle doit en outre englober toutes les couches d'un système. L'adoption d'une approche de la sécurité par couches conjuguée à une gestion et à une application de politiques efficaces permet d'offrir un ensemble de solutions de sécurité qui peuvent être modulaires, souples et évolutives.

Parmi les techniques actuellement utilisées pour la cybersécurité, on peut citer:

- la cryptographie: cette technologie puissante est utilisée dans un certain nombre de services de sécurité, notamment le chiffrement des données transmises ou stockées;
- les contrôles d'accès: le but est de limiter les possibilités offertes aux utilisateurs d'accéder aux informations présentes sur des serveurs ou des réseaux ainsi que d'utiliser, de visualiser et de modifier ces informations;
- l'intégrité des systèmes: le but est de garantir qu'un système et ses données ne sont pas modifiés ou altérés par des parties non autorisées ou de manière non autorisée;
- l'audit, la journalisation et la surveillance: ces techniques permettent aux administrateurs de système de collecter et d'examiner les journaux réseau pendant et après une attaque. Les données peuvent servir à évaluer l'efficacité de la stratégie de sécurité qui est mise en place dans le réseau;
- la gestion: cette technique permet aux administrateurs de système de revoir et de configurer les paramètres de sécurité sur leurs serveurs et réseaux. On peut utiliser des contrôles de gestion pour vérifier l'exactitude des paramètres des réseaux et des éléments associés.

3.6 Spécifications de sécurité du personnel et de sécurité physique

Les Recommandations UIT-T relatives à la sécurité portent essentiellement sur les aspects techniques des systèmes et des réseaux. Certains aspects de sécurité du personnel sont traités dans la Rec. UIT-T X.1051, *Lignes directrices pour la gestion de la sécurité des informations pour les organisations de télécommunication*. La sécurité physique est également une dimension très importante de la protection mais elle entre peu dans le cadre des travaux de l'UIT-T. Toutefois, des spécifications générales de sécurité physique sont énoncées dans la Rec. UIT-T X.1051 et la sécurité physique des installations extérieures est abordée dans les deux documents mentionnés ci-dessous.

En ce qui concerne la protection physique des installations extérieures, il s'agit notamment de faire en sorte que les matériels puissent résister aux menaces d'incendie, de catastrophe naturelle et de dommages intentionnels ou accidentels. Des méthodes de protection des composants, câbles, enceintes, armoires, etc., sont décrites dans les publications de l'UIT-T *Technologies des installations extérieures appliquées aux réseaux publics* (1991) et *Application des ordinateurs et des microprocesseurs à la fabrication, à l'installation et à la protection des câbles de télécommunication* (1999). Ces documents traitent également de la surveillance des systèmes afin de prévenir les dommages et indiquent la marche à suivre pour remédier aux problèmes et rétablir la fonctionnalité des systèmes le plus rapidement possible.

4. Architectures de sécurité

4 Architectures de sécurité

Les architectures de sécurité, et les modèles et cadres associés, constituent une structure et un contexte à l'intérieur desquels des normes techniques connexes peuvent être élaborées de manière cohérente. Au début des années 1980, il s'est avéré nécessaire de disposer d'un cadre dans lequel la sécurité pourrait être appliquée dans une architecture de communications en couches. C'est alors qu'a été définie l'*architecture de sécurité pour les systèmes ouverts* (Rec. UIT-T X.800), première d'une série de normes définissant des architectures pour les services et les mécanismes de sécurité. Ces travaux, menés en grande partie en collaboration avec l'ISO, ont conduit à d'autres normes, notamment sur des modèles et des cadres de sécurité qui spécifient comment des types de protection particuliers peuvent être appliqués dans des environnements particuliers.

Plus tard, il s'est avéré nécessaire de définir des architectures de sécurité génériques et des architectures de sécurité propres à certaines applications. C'est alors qu'a été définie l'*architecture de sécurité pour les systèmes assurant des communications de bout en bout* (Rec. UIT-T X.805), ainsi qu'un certain nombre d'architectures propres à certaines applications, par exemple la gestion de réseau, les communications entre homologues et les serveurs web mobiles. La Rec. UIT-T X.805, qui est décrite plus loin dans le présent chapitre, complète les autres Recommandations de la série X.800 en offrant des solutions de sécurité destinées à assurer la sécurité de réseau de bout en bout.

4.1 Architecture de sécurité pour les systèmes ouverts et normes associées

La première des architectures de sécurité pour les communications à avoir été normalisée a été l'architecture de sécurité pour les systèmes ouverts, définie dans la Rec. UIT-T X.800. Cette Recommandation définit les éléments d'architecture liés à la sécurité qui peuvent être appliqués en fonction des conditions dans lesquelles une protection est requise. Elle contient en particulier une description générale de services de sécurité et des mécanismes associés qui peuvent être utilisés pour assurer les services. Elle définit aussi, sur la base du modèle de référence de base à sept couches pour l'interconnexion des systèmes ouverts (OSI, *open systems interconnection*), les emplacements les plus appropriés (c'est-à-dire les couches) pour implémenter les services de sécurité.

La Rec. UIT-T X.800 porte uniquement sur les aspects visibles d'une voie de communication permettant aux systèmes d'extrémité de se transférer des informations en toute sécurité. Elle ne vise pas à spécifier des implémentations particulières et elle ne définit pas la marche à suivre pour évaluer la conformité d'une implémentation donnée à cette norme sur la sécurité ou à toute autre norme sur la sécurité. Elle ne précise pas non plus les mesures de sécurité additionnelles qui pourraient être nécessaires dans les systèmes d'extrémité pour prendre en charge les fonctionnalités de sécurité des communications.

L'architecture de sécurité définie dans la Rec. UIT-T X.800 a été élaborée spécifiquement pour les systèmes OSI, mais les concepts sous-jacents se sont avérés avoir une applicabilité et une acceptation beaucoup plus larges. La norme est particulièrement importante car elle représente le premier consensus à l'échelle internationale sur les définitions des services de sécurité de base (*authentification, contrôle d'accès, confidentialité des données, intégrité des données et non-répudiation*) ainsi que de services plus généraux (omniprésents) (*fonctionnalité de confiance, détection d'événements, audit de sécurité et reprise de sécurité, etc.*). Elle indique également les mécanismes de sécurité qui peuvent être utilisés pour fournir les services de sécurité. Avant l'élaboration de la Rec. UIT-T X.800, les avis étaient très partagés sur les services de sécurité de base nécessaires et sur les fonctionnalités exactes de chaque service. La Rec. UIT-T X.800 traduit un fort consensus international sur ces services.

L'intérêt et l'applicabilité générale de la Rec. UIT-T X.800 tiennent au fait que cette Recommandation représente un consensus important sur la signification des termes employés pour décrire les fonctionnalités

de sécurité, sur l'ensemble des services de sécurité nécessaires pour assurer la protection des communications de données et sur la nature de ces services de sécurité.

Au cours de l'élaboration de la Rec. UIT-T X.800, il s'est avéré nécessaire d'établir d'autres normes connexes sur la sécurité des communications. Un certain nombre de normes connexes et de Recommandations complémentaires relatives à l'architecture ont donc commencé à être mises au point. Certaines de ces Recommandations sont examinées ci-après.

4.2 Services de sécurité

Des cadres de sécurité ont été élaborés pour décrire de façon complète et cohérente chacun des services de sécurité définis dans la Rec. UIT-T X.800. Ils ont pour objet de définir tous les aspects liés à l'application des services de sécurité dans le contexte d'une architecture de sécurité particulière, y compris les éventuelles architectures de sécurité qui seront définies dans le futur. Ils visent essentiellement à assurer la protection des systèmes, des objets contenus dans les systèmes et de l'interaction entre les systèmes. Ils ne traitent pas de la marche à suivre pour construire des systèmes ou des mécanismes.

Les cadres portent à la fois sur les éléments de données et sur les séquences d'opérations (à l'exclusion des éléments de protocole) qui sont utilisés pour fournir des services de sécurité spécifiques. Ces services peuvent s'appliquer aux entités de système en communication ainsi qu'aux données échangées entre elles et gérées par elles.

L'aperçu des cadres de sécurité (Rec. UIT-T X.810) présente les différents cadres et décrit les concepts communs (domaines de sécurité, autorités de sécurité et politiques de sécurité) qui sont utilisés dans tous les cadres. Il décrit également un format de données générique qui peut être utilisé pour acheminer en toute sécurité les informations d'authentification et de contrôle d'accès.

L'authentification est l'attestation de l'identité revendiquée par une entité. Les entités incluent non seulement les utilisateurs humains, mais aussi les dispositifs, les services et les applications. L'authentification permet aussi d'attester qu'une entité ne tente pas d'usurper l'identité d'une autre entité ni de reprendre sans autorisation une communication précédente. La Rec. UIT-T X.800 définit deux formes d'authentification: *l'authentification de l'origine des données* (à savoir la confirmation que la source des données reçues est telle que déclarée) et *l'authentification de l'entité homologue* (à savoir la confirmation qu'une entité homologue d'une association est bien l'entité déclarée). Le *cadre d'authentification* (Rec. UIT-T X.811) définit les concepts de base de l'authentification, différentes classes de mécanismes d'authentification, les services correspondant à ces classes de mécanismes, les spécifications fonctionnelles que les protocoles doivent respecter pour prendre en charge ces classes de mécanismes et, enfin, les spécifications générales de gestion concernant l'authentification.

Le *contrôle d'accès* est la précaution prise contre l'utilisation non autorisée d'une ressource, y compris la précaution prise contre l'utilisation d'une ressource de façon non autorisée. Le contrôle d'accès garantit que seuls les personnes ou les dispositifs autorisés peuvent accéder aux éléments de réseau, aux informations stockées, aux flux d'informations, aux services et aux applications. Le *cadre de contrôle d'accès* (Rec. ITU-T X.812) décrit un modèle incluant tous les aspects du contrôle d'accès dans les systèmes ouverts, la relation avec les autres fonctions de sécurité (par exemple l'authentification et l'audit) et les spécifications de gestion concernant le contrôle d'accès.

La *non-répudiation* est la capacité d'empêcher les entités de nier ultérieurement qu'elles ont exécuté une action. Il s'agit d'établir une preuve qui puisse ensuite être utilisée pour rejeter les fausses déclarations. La Rec. UIT-T X.800 décrit deux formes de service de non-répudiation: la *non-répudiation avec preuve de remise*, qui sert à rejeter toute fausse déclaration d'un destinataire qui nie avoir reçu des données, et la *non-répudiation avec preuve d'origine*, qui sert à rejeter toute fausse déclaration d'un expéditeur qui nie avoir envoyé des données. Toutefois, dans un sens plus général, le concept de non-répudiation peut être appliqué à de nombreux contextes différents, notamment la non-répudiation de création, de soumission, de stockage, de transmission et de réception de données. Le *cadre de non-répudiation* (Rec. UIT-T X.813) élargit les

concepts des services de sécurité de non-répudiation décrits dans la Rec. UIT-T X.800 et sert de cadre pour la définition de ces services. En outre, il définit différents mécanismes de prise en charge de ces services et les spécifications générales de gestion concernant la non-répudiation.

La *confidentialité* est la propriété d'une information qui n'est ni communiquée, ni divulguée aux individus, entités ou processus non autorisés. Le service de confidentialité a pour objet de protéger les informations contre toute divulgation non autorisée. Le *cadre de confidentialité* (Rec. UIT-T X.814) porte sur la confidentialité des informations au moment de leur extraction, de leur transfert et de leur gestion. Il définit les concepts de base de la confidentialité, différentes classes de confidentialité et les fonctionnalités requises pour chaque classe de mécanismes de confidentialité. Il définit également les services de gestion et les services support requis ainsi que l'interaction avec les autres services et mécanismes de sécurité.

L'*intégrité des données* est la propriété de données qui n'ont pas été modifiées de façon non autorisée. En général, un service d'intégrité répond à la nécessité de garantir que les données ne sont pas corrompues ou, si elles le sont, que l'utilisateur est au courant de cette corruption. Le *cadre d'intégrité* (Rec. UIT-T X.815) porte sur l'intégrité des données au moment de leur extraction, de leur transfert et de leur gestion. Il définit les concepts de base de l'intégrité, différentes classes de mécanismes d'intégrité et les fonctionnalités, spécifications de gestion et services connexes nécessaires pour chaque classe de mécanismes. (Il est à noter que, bien que les normes sur les architectures de sécurité portent essentiellement sur l'intégrité des données, d'autres aspects de l'intégrité, par exemple l'intégrité des systèmes, sont également importants pour la sécurité.)

4.3 Architecture de sécurité pour les systèmes assurant des communications de bout en bout

En 2003, après un examen approfondi de l'architecture de sécurité pour les réseaux, la Rec. UIT-T X.805, *Architecture de sécurité pour les systèmes assurant des communications de bout en bout*, a été approuvée. Cette architecture, qui reprend et élargit certains concepts de la Rec. UIT-T X.800 et les cadres de sécurité présentés ci-dessus, peut être appliquée à divers types de réseau et ne dépend pas de la technologie.

4.3.1 Éléments de l'architecture UIT-T X.805

L'architecture X.805 est définie sur la base de trois principaux concepts pour les réseaux de bout en bout: les couches, les plans et les dimensions de sécurité. On adopte une approche hiérarchique de subdivision des spécifications de sécurité entre les couches et les plans de manière à assurer la sécurité de bout en bout en définissant des mesures de sécurité dans chacune des dimensions pour prendre en compte les menaces spécifiques. La Figure 1 illustre les éléments de cette architecture.

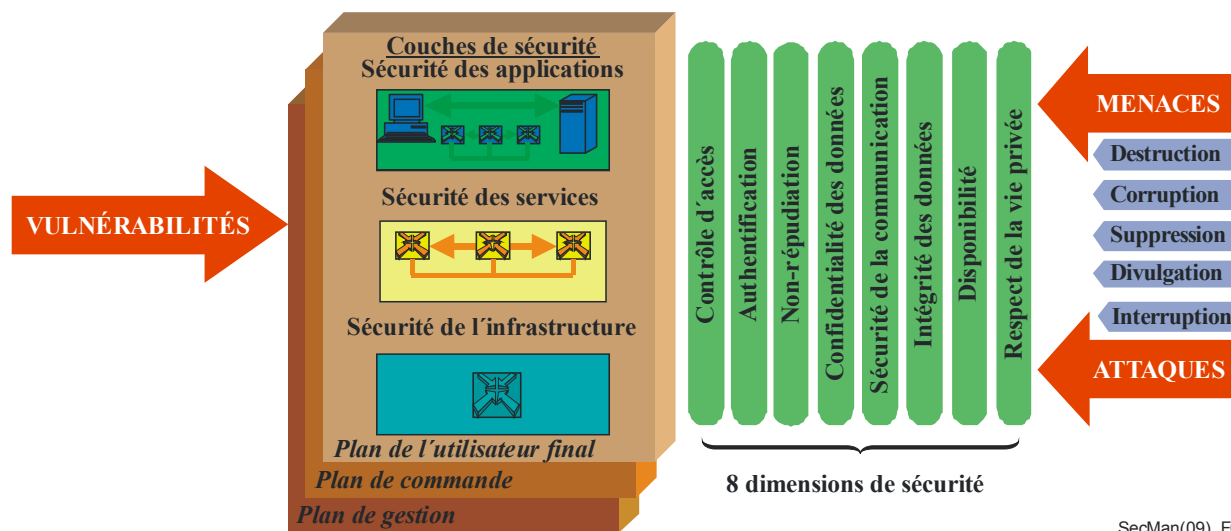


Figure 1 – Éléments de l'architecture de sécurité (Rec. UIT-T X.805)

SecMan(09)_F01

Dans la Rec. UIT-T X.805, une *dimension de sécurité* est un ensemble de mesures de sécurité conçues pour prendre en compte un aspect particulier de la sécurité du réseau. Les services de sécurité de base de la Rec. UIT-T X.800 (*contrôle d'accès, authentification, confidentialité des données, intégrité des données et non-répudiation*) concordent avec les fonctionnalités des *dimensions de sécurité* correspondantes de la Rec. UIT-T X.805 (illustrées sur la Figure 1). En outre, la Rec. UIT-T X.805 introduit trois dimensions (*sécurité de la communication, disponibilité et respect de la vie privée*) qui ne figurent pas dans la Rec. UIT-T X.800. Ces dimensions offrent une protection de réseau complémentaire contre toutes les principales menaces de sécurité. Elles ne sont pas limitées au réseau mais couvrent aussi les applications et les informations des utilisateurs finals. Les dimensions de sécurité s'appliquent aux fournisseurs de service ou entreprises qui offrent des services de sécurité à leurs clients.

Les huit dimensions de sécurité définies dans la Rec. UIT-T X.805 sont les suivantes:

- la dimension *contrôle d'accès*, qui permet d'assurer la protection contre toute utilisation non autorisée de ressources de réseau et de garantir que seuls les personnes ou les dispositifs autorisés peuvent accéder aux éléments de réseau, aux informations stockées, aux flux d'informations, aux services et aux applications;
- la dimension *authentification*, qui sert à confirmer les identités des entités qui communiquent, qui permet de garantir la validité des identités déclarées des entités en communication (par exemple, une personne, un dispositif, un service ou une application) et qui permet d'attester qu'une entité ne tente pas d'usurper l'identité d'une autre entité ou de reprendre sans autorisation une précédente communication;
- la dimension *non-répudiation*, qui permet d'empêcher une personne ou une entité de nier avoir exécuté une action particulière liée aux données, grâce à la fourniture de diverses preuves d'actions dans le réseau (par exemple une preuve d'obligation, d'intention ou d'engagement; une preuve d'origine des données, une preuve de propriété ou une preuve d'emploi de ressources). Elle permet aussi à une preuve d'être présentée à une entité tierce et d'être utilisée pour prouver qu'un événement ou une action a eu lieu;
- la dimension *confidentialité des données*, qui permet de protéger les données contre toute divulgation non autorisée et de garantir que le contenu des données ne pourra être compris par des entités non autorisées;
- la dimension *sécurité de la communication*, qui permet de garantir que les informations ne sont acheminées qu'entre les points d'extrémité autorisés, autrement dit que les informations ne sont ni déviées ni interceptées au cours de leur acheminement entre ces points;

- la dimension *intégrité des données*, qui permet de garantir que les données sont protégées contre toute modification, suppression, création et reproduction non autorisées et de fournir une alerte au cas où des activités pourraient compromettre l'intégrité des données;
- la dimension *disponibilité*, qui permet de garantir qu'il n'y a pas déni de l'accès autorisé aux éléments de réseau, aux informations stockées, aux flux d'informations, aux services et aux applications en raison d'événements ayant une incidence sur le réseau; et
- la dimension *respect de la vie privée*, qui permet d'assurer la protection des informations qui pourraient être obtenues à partir de l'observation des activités dans le réseau. On peut citer par exemple les sites web qu'un utilisateur a visités, l'emplacement géographique d'un utilisateur, ainsi que les adresses IP et les noms DNS des dispositifs présents dans le réseau d'un fournisseur de service.

Comme indiqué sur la Figure 1, en plus des dimensions de sécurité, la Rec. UIT-T X.805 définit trois couches de sécurité et trois plans. Afin de disposer d'une solution de sécurité de bout en bout, les dimensions de sécurité doivent être appliquées à une hiérarchie de groupes d'équipements et d'installations de réseau, qu'on désigne comme étant les *couches de sécurité*. Un *plan de sécurité* représente un certain type d'activité dans le réseau, protégée par des dimensions de sécurité. Chaque plan de sécurité représente un type d'activité protégée dans le réseau.

Les couches de sécurité définissent les spécifications qui s'appliquent aux éléments de réseau et aux systèmes ainsi qu'aux services et applications associés à ces éléments. La définition des couches présente notamment pour avantage de pouvoir réutiliser ces couches dans différentes applications pour assurer la sécurité de bout en bout. Les vulnérabilités au niveau de chaque couche sont différentes et il faut donc définir différentes contre-mesures pour répondre aux besoins de chaque couche. Les trois couches sont les suivantes:

- la couche *infrastructure*, qui comprend les installations de transmission de réseau et les différents éléments de réseau. Elle comprend notamment les routeurs, commutateurs et serveurs ainsi que les liaisons de communication qui les relient;
- la couche *services*, qui définit la sécurité des services de réseau qui sont offerts aux clients. Ces services vont des offres de connexion de base telles que les services de lignes louées aux services à valeur ajoutée tels que la messagerie instantanée; et
- la couche *applications*, qui définit les spécifications relatives aux applications de réseau utilisées par les clients. Ces applications peuvent être aussi simples que la messagerie électronique ou aussi complexes que, par exemple, la visualisation collaborative, pour laquelle des transferts vidéo haute définition sont opérés dans des domaines comme ceux de l'exploration pétrolière ou de la conception d'automobiles.

Les plans de sécurité visent à répondre aux besoins de sécurité particuliers associés aux activités de gestion de réseau, aux activités de signalisation et de commande de réseau et aux activités d'utilisateur final. Les réseaux devraient être conçus de manière à ce que les événements se produisant sur un plan de sécurité soient isolés des autres plans de sécurité.

Les plans de sécurité sont les suivants:

- le plan de *gestion*, qui se rapporte aux activités d'exploitation, d'administration, de maintenance et de configuration, par exemple la configuration d'un utilisateur ou d'un réseau;
- le plan de *commande*, qui est associé aux aspects de signalisation pour l'établissement (et la modification) de la communication de bout en bout dans le réseau, quels que soient le support ou la technologie utilisés dans le réseau; et
- le plan de *utilisateur final*, dans lequel il s'agit d'assurer la sécurité d'accès au réseau et d'utilisation du réseau par les abonnés. Il s'agit aussi d'assurer la protection des flux de données d'utilisateur final.

L'architecture UIT-T X.805 peut servir de guide pour élaborer des politiques de sécurité, des architectures techniques et des plans d'intervention en cas d'incident et de retour à la normale. Elle peut aussi servir de base à une évaluation de la sécurité. Dès qu'un programme de sécurité a été mis en place, il doit être tenu à jour compte tenu de l'évolution permanente de l'environnement des menaces. L'architecture de sécurité X.805 peut faciliter la tenue à jour d'un programme de sécurité, en permettant de veiller à ce que les modifications apportées au programme prennent en considération les dimensions de sécurité applicables dans chaque couche et chaque plan de sécurité.

La Rec. UIT-T X.805 porte sur une architecture de sécurité pour les réseaux, mais certains concepts peuvent être élargis aux dispositifs d'utilisateur final. Cet aspect est pris en compte dans la Rec. UIT-T X.1031, *Rôle des utilisateurs finals et des réseaux de télécommunication dans l'architecture de sécurité*.

4.3.2 Disponibilité du réseau et de ses composants

La disponibilité du réseau est un aspect important de la sécurité des TIC. Comme indiqué plus haut, la dimension de sécurité *disponibilité* de la Rec. UIT-T X.805 a pour objet de garantir la continuité de service et de garantir l'accès aux éléments de réseau, aux informations et aux applications lorsque cet accès est autorisé. Les solutions de retour à la normale après une catastrophe sont comprises dans cette dimension.

La couche de sécurité infrastructure comprend les installations de transmission de réseau et les différents éléments de réseau protégés par les dimensions de sécurité. Elle représente les composants fondamentaux des réseaux, leurs services et applications. Elle comprend notamment les routeurs, commutateurs et serveurs ainsi que les liaisons de communication qui les relie.

Les spécifications fonctionnelles et opérationnelles destinées à limiter les risques d'indisponibilité des ressources de réseau et d'en réduire les conséquences sont nombreuses et variées. Parmi les nombreux facteurs à prendre en considération, on peut citer les caractéristiques d'erreurs, la limitation des encombrements, la signalisation des défaillances et les mesures correctives. La Recommandation UIT-T G.827, *Paramètres et objectifs de disponibilité pour les conduits numériques internationaux de bout en bout à débit constant*, définit les paramètres et objectifs de disponibilité pour les conduits numériques internationaux de bout en bout à débit constant ou des éléments de ces conduits. Ces paramètres sont indépendants du type de réseau physique prenant en charge le conduit de bout en bout. L'Annexe A de la Rec. UIT-T G.827 donne des indications détaillées sur les méthodes permettant d'évaluer la disponibilité de bout en bout et donne des exemples de topologies de conduit et de calculs de disponibilité de conduit de bout en bout. D'autres Recommandations traitent de la qualité de fonctionnement des réseaux, notamment: la Rec. UIT-T G.1000, *Qualité de service des communications: cadre et définitions*, la Rec. UIT-T G.1030, *Evaluation de la qualité de fonctionnement de bout en bout dans les réseaux IP pour les applications de transmission de données*, la Rec. UIT-T G.1050, *Modèle de réseau pour l'évaluation de la qualité de transmission multimédia sur protocole Internet* et la Rec. UIT-T G.1081, *Points de surveillance de la qualité de fonctionnement pour la TVIP*.

4.4 Guide de mise en œuvre

Les normes de l'UIT-T sur l'architecture de sécurité font toutes partie de la série UIT-T X.800-849 de Recommandations sur la sécurité. Un guide de mise en œuvre est fourni dans un supplément à cette série de Recommandations (X.Sup3, série UIT-T X.800-X.849 – *Lignes directrices pour la mise en œuvre de la sécurité dans les systèmes et dans les réseaux*). Ce supplément énonce des lignes directrices concernant les activités critiques pendant le cycle de vie de la sécurité dans les réseaux. Quatre domaines sont traités: politique de sécurité technique; identification des actifs hiérarchiques; menaces, vulnérabilités et solutions d'atténuation en fonction des actifs hiérarchiques; et évaluation de la sécurité. Les lignes directrices et les tableaux associés visent à permettre de mettre en place de façon systématique une planification, une analyse et une évaluation de la sécurité dans les réseaux.

4.5 Architectures propres à certaines applications

Le présent paragraphe expose certains aspects des architectures applicables à certaines applications.

4.5.1 Communications entre homologues

Le P2P (*peer-to-peer*, homologue à homologue) est une instantiation d'architectures de réseau dans laquelle tous les homologues ont une autorité et des attributions équivalentes, par opposition au modèle client/serveur. Dans le cas des communications P2P, un homologue peut être à la fois le serveur et le client. Lorsque des données ou des messages sont échangés dans un réseau P2P, un homologue communique directement avec d'autres homologues. Etant donné que le trafic et le traitement sont l'affaire de chaque homologue, le réseau P2P n'a pas besoin d'une grande performance en termes de puissance de traitement ou d'une grande largeur de bande.

Le réseau P2P est superposé sur le réseau de télécommunication et l'Internet. Il s'appuie non pas sur des ressources centralisées classiques mais sur la connectivité entre les nœuds et sur la puissance de traitement et la capacité de stockage disponibles dans chaque nœud.

Avec les progrès rapides enregistrés dans les réseaux de télécommunication et la technologie informatique, un nombre beaucoup plus grand d'informations et de ressources informatiques peuvent être disponibles dans des nœuds répartis plutôt qu'à partir d'un nombre limité de serveurs centralisés.

Les réseaux P2P sont généralement utilisés pour raccorder des nœuds au moyen de connexions ad hoc. Leurs applications sont très nombreuses. Le partage de fichiers contenant des données en format numérique (audio, vidéo, texte, etc.) est très courant. La technologie P2P est également utilisée pour des communications en temps réel (téléphonie par exemple).

4.5.1.1 Architecture de sécurité et opérations pour les réseaux entre homologues

Une architecture générale relative à la sécurité qui peut être appliquée dans divers réseaux P2P est décrite dans la Recommandation UIT-T X.1162.

La Figure 2 illustre une architecture de service P2P de base. Les informations traitées par chaque homologue sont échangées directement entre les utilisateurs. Comme il n'existe pas de serveur central pour le stockage des informations, chaque homologue doit trouver quels homologues possèdent les données cibles avant de pouvoir récupérer ces données. De plus, chaque homologue doit permettre aux autres homologues d'accéder à ses données avant que l'échange de données puisse avoir lieu.

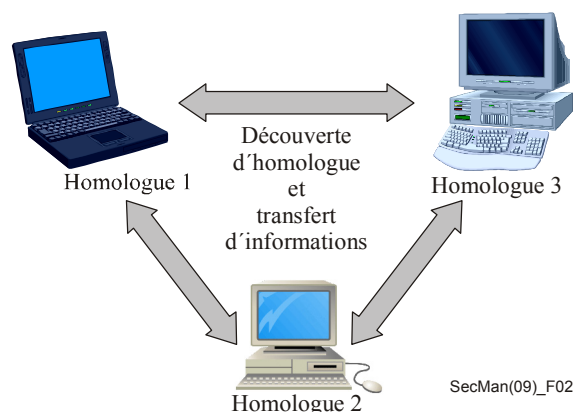


Figure 2 – Architecture de service P2P

La Figure 3 illustre l'architecture de réseau P2P physique et logique. Dans le réseau P2P physique, un utilisateur peut accéder aux services P2P au moyen d'un dispositif. Le terme "homologue" désigne généralement un utilisateur ou un dispositif de l'utilisateur. On distingue les types suivants de connexion entre les entités dans un réseau P2P:

- connexion avec un homologue intra-domaine;
- connexion avec un homologue inter-domaines; et
- connexion avec un fournisseur de service homologue situé dans un autre domaine de réseau.

La Figure 3 illustre également l'architecture de réseau P2P logique en tant que réseau virtuel sur la strate de transport. On part du principe que le fonctionnement de chaque homologue n'est pas limité par l'architecture de réseau physique et qu'un homologue peut communiquer avec n'importe quel autre homologue quel que soit son emplacement (avec l'aide d'un super-homologue, si nécessaire). La structure du réseau entre homologues est subdivisée en deux strates: la strate de superposition P2P et la strate de transport. La strate de transport est chargée du transfert des paquets en provenance ou à destination de la couche supérieure et la strate de superposition est chargée de la fourniture des services P2P.

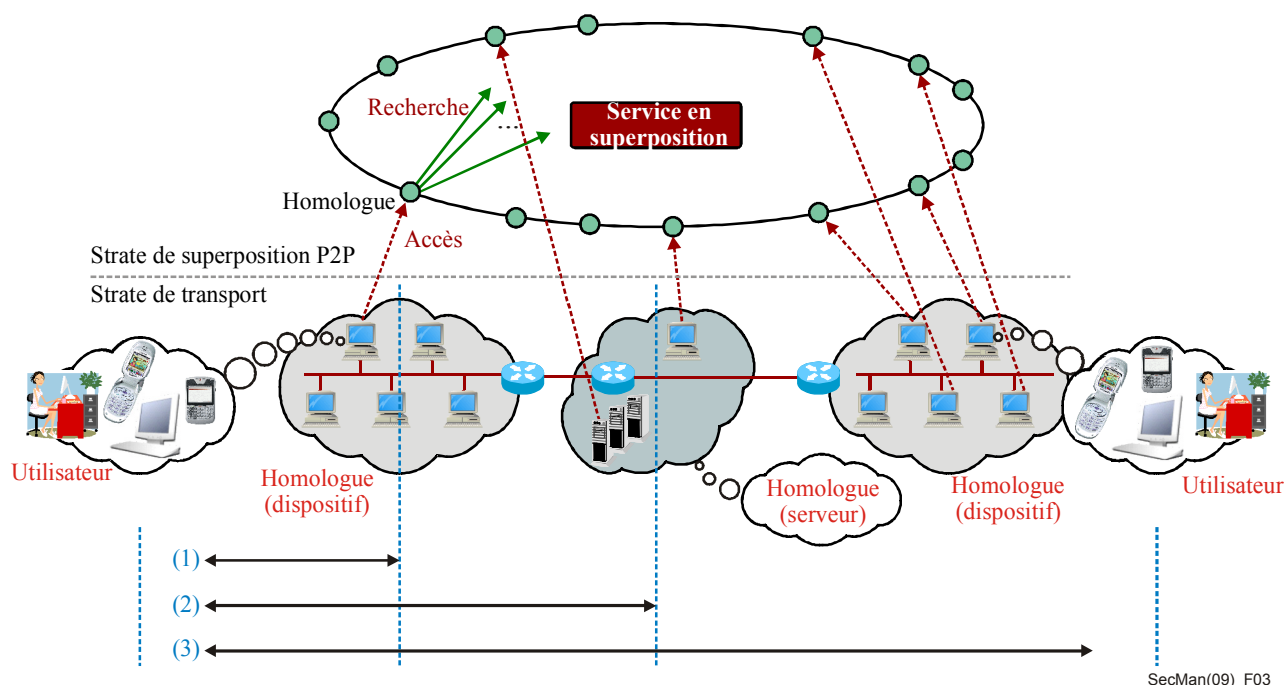


Figure 3 – Modèle de référence de l'architecture du réseau P2P

4.5.1.2 Cadre général des communications sécurisées entre homologues

Les spécifications de sécurité pour les réseaux P2P ainsi que les services et mécanismes nécessaires pour satisfaire ces spécifications font l'objet de la Recommandation UIT-T X.1161, *Cadre général des communications sécurisées entre homologues*.

Les menaces qui pèsent sur les communications P2P sont notamment les suivantes: écoute clandestine, brouillage, injection & modification, accès non autorisé, répudiation, attaques de l'intercepteur (*man-in-the-middle*) et attaques Sybil. Les mesures permettant de lutter contre les menaces P2P sont indiquées dans le Tableau 3.

Tableau 3 – Relation entre les spécifications de sécurité P2P et les contremesures

Fonctions Spécifications	Chiffrement	Echange de clés	Signature numérique	Gestion de la confiance	Contrôle d'accès	Mécanisme d'intégrité des données	Echange pour authentification	Notarisation	Routage sécurisé	Mécanisme de contrôle du trafic	Attribution d'un identifiant
Authentification de l'utilisateur	X	X	X	X	X		X				X
Anonymat	X			X							X
Respect de la vie privée	X				X		X				
Intégrité des données	X	X	X		X	X	X				
Confidentialité des données	X	X			X		X				
Contrôle d'accès					X		X				X
Non-répudiation			X				X	X			X
Utilisabilité					X						
Disponibilité					X		X		X	X	
Traçabilité			X						X		X
Contrôle du trafic		X								X	

4.5.2 Architecture de sécurité des messages dans l'environnement des services web mobiles

L'architecture de sécurité des messages dans l'environnement des services web mobiles et les scénarios associés sont décrits dans la Recommandation UIT-T X.1143, *Architecture de sécurité des messages dans l'environnement des services web mobiles*. Cette norme définit:

- une architecture de sécurité des messages qui repose sur des mécanismes de politique de service web appropriés;
- des mécanismes d'interfonctionnement et des scénarios de service entre les applications qui prennent en charge toute la pile de protocoles de sécurité des services web et les applications existantes qui ne prennent pas en charge toute cette pile;
- des mécanismes d'authentification, d'intégrité et de confidentialité des messages;
- un mécanisme de filtrage des messages reposant sur leur contenu; et
- une architecture de sécurité des messages de référence et des scénarios pour les services de sécurité.

La Figure 4 illustre l'architecture de sécurité UIT-T X.1143 pour les services web mobiles.

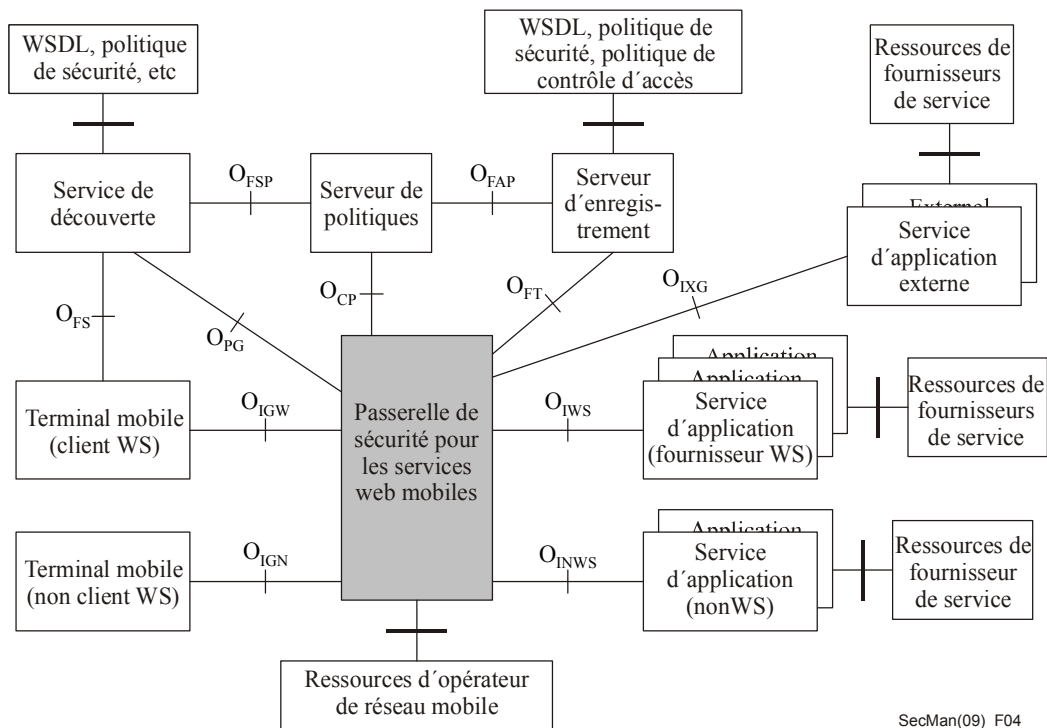


Figure 4 – Architecture de sécurité pour les services web mobiles

L'architecture de sécurité comprend:

- des terminaux mobiles, qui sont des clients des services web mobiles;
- une passerelle de sécurité pour les services web mobiles (MWSSG). Toutes les demandes émanant de clients mobiles sont envoyées à la passerelle MWSSG, qui applique un contrôle d'accès;
- le serveur de politiques, qui gère les politiques de sécurité relatives au traitement sécurisé des messages et les politiques de contrôle d'accès aux messages;
- le service d'application, qui offre divers services à valeur ajoutée aux clients;
- le service de découverte, qui stocke les informations d'interface pour les services d'application et les politiques de sécurité associées pour l'accès aux services d'application par les clients; et
- le serveur d'enregistrement, qui réside dans le domaine interne de l'opérateur mobile et gère les informations d'interface pour les services d'application, les politiques de sécurité associées pour l'accès aux services d'application par les clients et les politiques de contrôle d'accès relatives aux services cibles.

4.6 Autres architectures et modèles de sécurité de réseau

D'autres aspects des architectures de sécurité de réseau sont abordés plus loin dans le texte. On pourra en particulier se reporter aux paragraphes 7.2 Architecture de gestion de réseau, 8.1 Sécurité des réseaux de prochaine génération (NGN), 8.4.1 Architecture IPCablecom, 8.5.1 Architecture IPCablecom2 et 9.2 TVIP.

5. Aspects de gestion de la sécurité

5 Aspects de gestion de la sécurité

La gestion de la sécurité est un vaste sujet qui englobe de nombreuses activités associées au contrôle et à la protection de l'accès aux ressources des systèmes et des réseaux, à la surveillance des événements, à la notification, aux politiques et à l'audit, ainsi qu'à la gestion des informations relatives à ces fonctions et activités. Le présent chapitre porte sur certaines activités génériques de gestion de la sécurité. Les activités de gestion de la sécurité associées à la sécurisation de l'infrastructure de réseau sont examinées dans le chapitre 7.

5.1 Gestion de la sécurité des informations

Tout comme les autres actifs, les informations sont essentielles pour les activités d'une organisation. Elles peuvent être imprimées, stockées sous forme électronique, transmises par courrier, communiquées par voie électronique, affichées dans des films, communiquées dans des conversations ou acheminées par d'autres moyens. Quelle que soit leur forme ou leur fonctionnalité, ou le moyen utilisé pour les partager ou les stocker, les informations devraient toujours bénéficier d'une protection appropriée.

En cas de violation de la sécurité des informations, par exemple en cas d'accès non autorisé au système de traitement de l'information d'une organisation, l'organisation peut subir des dommages importants. Il est donc essentiel pour une organisation de garantir la sécurité de ses informations en mettant en place un processus structuré de gestion de la sécurité.

On parvient à gérer efficacement la sécurité des informations en mettant en place un ensemble de contrôles appropriés. Ces contrôles, qui s'appliquent aux installations de télécommunication, services et applications, doivent être établis, mis en œuvre, surveillés, revus et améliorés en permanence. L'absence de déploiement de contrôles de sécurité efficaces peut empêcher une organisation de remplir ses objectifs de sécurité et les objectifs propres à ses activités.

Les organisations de télécommunication dont les installations sont utilisées par les abonnés pour le traiter d'informations (données personnelles, données confidentielles, données sensibles, etc.) doivent garantir un niveau de protection approprié pour empêcher toute compromission des informations, autrement dit, elles doivent établir un système de gestion de la sécurité des informations (ISMS) efficace.

La spécification ISMS la plus largement reconnue est celle qui est définie dans la série ISO/CEI 27000 de normes ISMS qui contient des normes sur les fondements du système ISMS, les spécifications, un code de bonne pratique, un guide de mise en œuvre et des aspects connexes. L'UIT-T et l'ISO/CEI ont élaboré conjointement la Rec. UIT-T X.1051 | ISO/CEI 27011, *Lignes directrices pour la gestion de la sécurité des informations pour les organisations de télécommunication*, sur la base de la norme ISO/CEI 27002 (Code de bonne pratique pour la gestion de la sécurité des informations).

La Recommandation UIT-T X.1051 établit des lignes directrices et des principes généraux pour instaurer, mettre en œuvre, maintenir et améliorer la gestion de la sécurité des informations dans les organisations de télécommunication et donne des indications de base pour la mise en œuvre de la gestion de la sécurité des informations afin de garantir la confidentialité, l'intégrité et la disponibilité des installations et services de télécommunication. Des indications destinées tout particulièrement au secteur des télécommunications sont données sur les aspects suivants:

- organisation de la sécurité des informations;
- gestion des actifs;
- sécurité des ressources humaines;
- sécurité physique et environnementale;

- gestion des communications et gestion de l'exploitation;
- contrôle d'accès;
- acquisition de systèmes d'information;
- développement et maintenance;
- gestion des incidents; et
- gestion de la continuité des activités.

En plus de l'application des objectifs et contrôles de sécurité décrits dans la Rec. UIT-T X.1051, les organisations de télécommunication doivent aussi tenir compte de ce qui suit:

- les informations relatives aux organisations de télécommunication doivent être protégées contre toute divulgation non autorisée. Ainsi, l'existence, le contenu, l'origine, la destination et les date et heure des informations communiquées ne doivent pas être divulguées;
- la mise en place et l'utilisation des installations de télécommunication devraient être contrôlées afin de garantir l'authenticité, l'exactitude et l'exhaustivité des informations transmises, relayées ou reçues par câble, par voie hertzienne ou par toute autre méthode; et
- tout accès à des informations et installations de télécommunication et au support utilisé pour la fourniture de services de communication doit être autorisé et ne devrait être accordé que lorsque c'est nécessaire. Dans le prolongement des dispositions relatives à la disponibilité, les organisations de télécommunication devraient donner la priorité aux communications essentielles en cas d'urgence et se conformer aux réglementations applicables.

La gestion de la sécurité des informations dans les organisations de télécommunication est indispensable quel que soit le support ou le mode de transmission. Si la gestion de la sécurité des informations n'est pas mise en œuvre correctement, les risques associés à l'utilisation du système seront accrus.

Pour la fourniture de leurs services, les organisations de télécommunication font office d'intermédiaire dans le transfert des données opéré par d'autres organisations ou par des particuliers. Il faut donc tenir compte du fait que les installations de traitement de l'information d'une organisation de télécommunication sont accessibles et utilisées non seulement par ses propres employés et contractuels, mais aussi par divers utilisateurs en dehors de l'organisation.

Sachant que les services et installations de télécommunication peuvent être utilisés en partage et/ou faire l'objet d'une interconnexion avec d'autres fournisseurs de service, l'infrastructure de réseau, les services, les applications et les installations doivent absolument tous être pris en compte pour la gestion de la sécurité des informations dans les organisations de télécommunication.

5.2 Gestion des risques

Par gestion des risques, on entend l'évaluation et la quantification des risques et la prise de mesures pour faire en sorte que les risques résiduels soient inférieurs à un niveau acceptable déterminé à l'avance. La gestion des risques a été présentée brièvement dans le chapitre 3 dans la discussion sur la Recommandation UIT-T X.1205, *Présentation générale de la cybersécurité*. Des lignes directrices plus détaillées sont énoncées dans la Recommandation UIT-T X.1055, *Guide concernant la gestion des risques et les profils de risques pour les organisations de télécommunication*, qui décrit des processus et des techniques permettant de réduire les risques pour la sécurité des informations. Ces processus et techniques peuvent être utilisés pour évaluer les spécifications de sécurité des télécommunications et les risques associés et pour faciliter le choix, la mise en œuvre et la mise à jour de contrôles appropriés pour maintenir le niveau de sécurité requis.

De nombreuses méthodes spécifiques de gestion des risques ont été élaborées. La Recommandation UIT-T X.1055 énonce les critères à utiliser pour évaluer et choisir des méthodes appropriées pour une organisation de télécommunication. Cependant, elle ne propose pas de méthode spécifique de gestion des risques.

Le processus de gestion des risques est illustré sur la Figure 5.

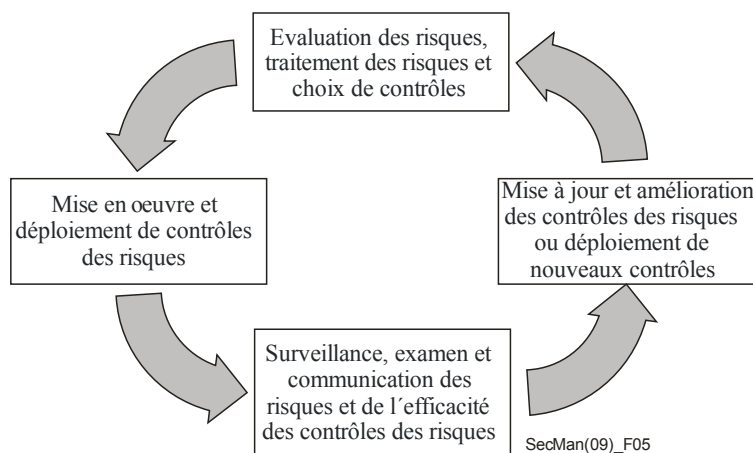


Figure 5 – Processus de gestion des risques (UIT-T X.1055)

Des profils de risques sont utilisés pour guider le processus global de gestion des risques. Plus précisément, ils sont utilisés pour faciliter la prise de décision et le classement des risques par ordre de priorité selon leur caractère critique et pour aider à déterminer l’attribution des ressources et les contremesures. Ils peuvent aussi être utiles pour élaborer des paramètres appropriés et être utilisés avec d’autres outils (méthodes d’analyse d’écart par exemple). La Recommandation UIT-T X.1055 donne des indications pour définir des profils de risques et contient un modèle de profil ainsi que quelques exemples de profils de risques.

5.3 Prise en charge des incidents

La gestion de la sécurité repose sur la détection des incidents relatifs à la sécurité, leur prise en charge et la diffusion d’informations au sujet de ces incidents et ce, de façon systématique. Si tous ces incidents ne sont pas évalués et pris en charge correctement, les organisations seront vulnérables aux attaques ultérieures, qui pourront être plus graves.

En l’absence de procédure établie de prise en charge des incidents, lorsqu’un incident relatif à la sécurité est détecté, il risque de ne pas être signalé ou analysé correctement. Il se peut aussi qu’il n’existe pas de procédures pour faire remonter la signalisation ou obtenir une assistance technique ou des orientations de gestion, même si les problèmes posés par ces incidents ont souvent des ramifications qui sortent du cadre des services informatiques ou des réseaux. Les incidents peuvent par exemple avoir des conséquences juridiques, financières ou sur le plan de la réputation ou peuvent relever de l’application de la loi. L’absence de procédures efficaces de prise en charge des incidents peut conduire à effectuer une réparation rapide ou à adopter une solution de rechange, au lieu de traiter, documenter et signaler correctement le problème, auquel cas il existe un risque pour que des problèmes plus graves se produisent ultérieurement.

Les organisations étant de plus en plus sensibles à la nécessité d’une gestion de la sécurité méthodique et efficace pour leurs réseaux et leurs activités, la prise en charge des incidents devient de plus en plus courante. Une équipe ou un groupe correctement formé et mandaté peut prendre en charge les incidents de sécurité promptement et correctement.

Afin d’être en mesure de prendre en charge et de signaler correctement les incidents, il est nécessaire de comprendre comment ils sont détectés, gérés et résolus. L’établissement d’une structure générale de prise en charge des incidents (à savoir, les incidents physiques, administratifs ou organisationnels, et logiques) permet d’obtenir une image générale de la nature et du déroulement d’un incident. La Recommandation UIT-T E.409, *Organisation en cas d’incident et prise en charge des incidents relatifs à la sécurité: lignes directrices destinées aux organisations de télécommunication*, donne un aperçu général et des orientations

afin de prévoir l'organisation de la détection et de la prise en charge des incidents relatifs à la sécurité. Elle est générique par nature et ne traite pas de spécifications applicables à des réseaux particuliers.

Il est essentiel de disposer d'une terminologie uniforme pour la signalisation et la prise en charge d'un incident. L'emploi d'une terminologie différente peut conduire à des malentendus, qui peuvent empêcher qu'un incident de sécurité reçoive l'attention appropriée ou la prise en charge rapide qui sont nécessaires pour le contenir et pour éviter qu'il ne se reproduise. De plus, la définition de ce qui est considéré comme un incident peut varier suivant les métiers, les organisations et les personnes. La Rec. UIT-T E.409 tente de normaliser la terminologie applicable à la détection et à la prise en charge des incidents et d'établir un classement des incidents en fonction de leur gravité (voir la Figure 6).

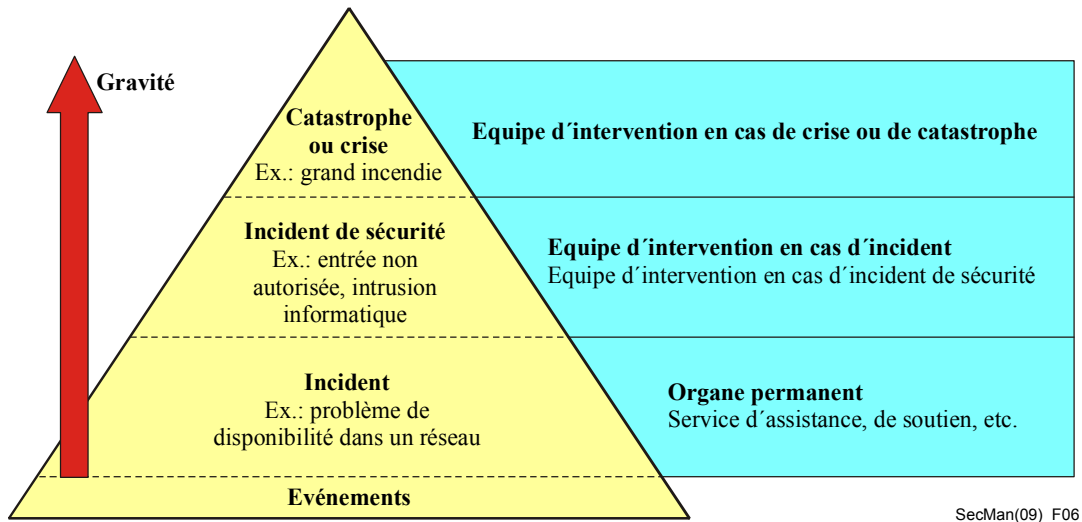


Figure 6 – Pyramide des événements et des incidents (UIT-T E.409)

La Recommandation UIT-T E.409 définit aussi une structure de prise en charge des incidents (illustrée sur la Figure 7) et établit des procédures pour la détection, le classement, l'évaluation, la prise en charge et le suivi des incidents.

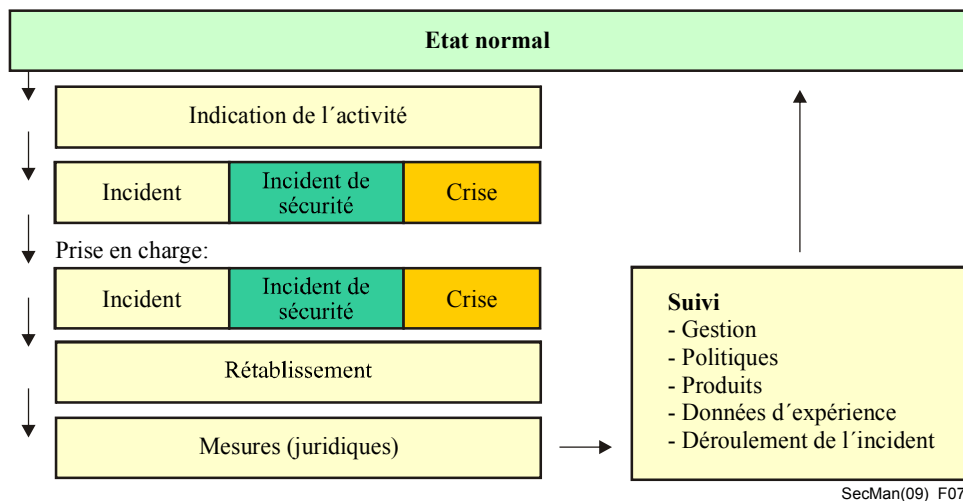


Figure 7 – Structure de prise en charge des incidents (UIT-T E.409)

La Rec. UIT-T X.1056, *Lignes directrices relatives à la gestion des incidents de sécurité dans les télécommunications*, qui a été approuvée récemment, s'appuie sur les indications données dans la Rec. UIT-T E.409. Les organisations de télécommunication doivent disposer de processus établis tant pour prendre en charge les incidents que pour éviter qu'ils se reproduisent. La Rec. UIT-T X.1056 décrit cinq processus de gestion des incidents de haut niveau ainsi que la relation avec la gestion de la sécurité (voir la Figure 8 et la Figure 9).

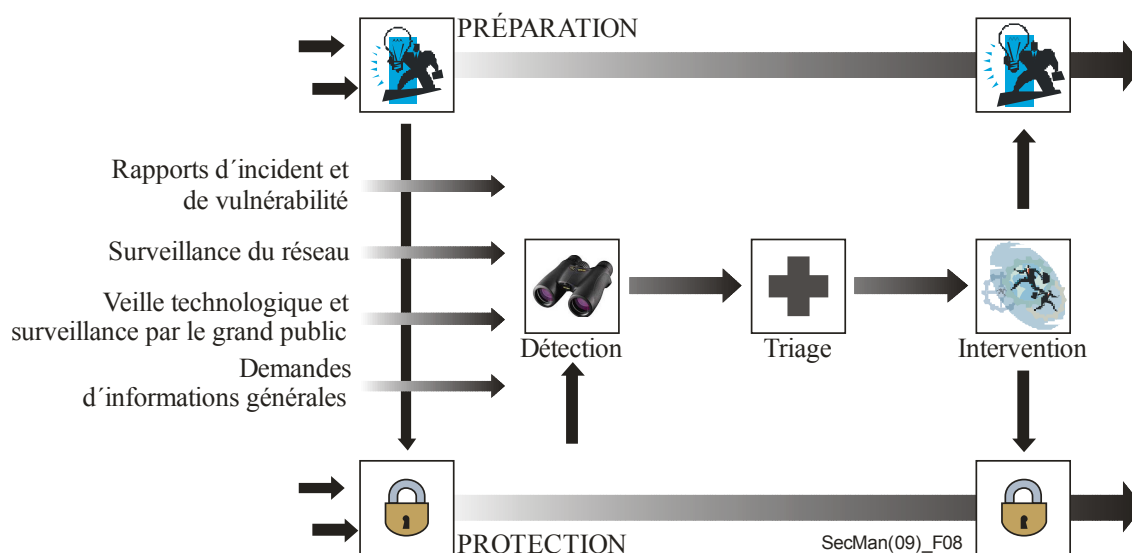


Figure 8 – Cinq processus de gestion des incidents de haut niveau

(Source: Executive Overview of SEI MOSAIC: Technical Report CMU/SEI-2004-TR-015 – Defining Incident Management Processes for CSIRTs: A Work in Progress)

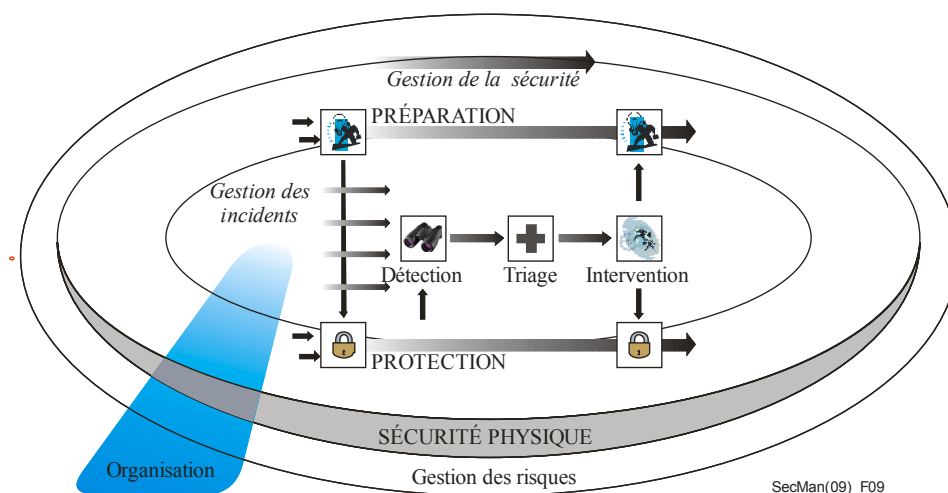


Figure 9 – Comparaison de la gestion des incidents et de la gestion de la sécurité

(Source: Executive Overview of SEI MOSAIC: Technical Report CMU/SEI-2004-TR-015 – Defining Incident Management Processes for CSIRTs: A Work in Progress)

Par ailleurs, la Rec. UIT-T X.1056 décrit différents services réactifs, proactifs et de gestion de la qualité de la sécurité qu'une équipe de gestion des incidents de sécurité peut offrir.

6. L'annuaire, authentification et gestion d'identité

6 L'annuaire, authentification et gestion d'identité

Le terme anglais "directory" désigne généralement un répertoire, autrement dit un ensemble organisé d'informations ou de fichiers qui peuvent être interrogés pour obtenir des informations particulières. Au sein de l'UIT-T et, plus généralement, dans le cadre de la normalisation de la sécurité et des télécommunications, le terme anglais « directory » désigne un *annuaire*, autrement dit un répertoire d'informations reposant sur la série de Recommandations UIT-T X.500, qui ont été élaborées conjointement avec l'ISO/CEI. L'annuaire, qui est présenté dans la Recommandation UIT-T X.500, *L'annuaire: aperçu général des concepts, modèles et services*, et décrit en détail dans les Recommandations UIT-T X.501, *L'annuaire: les modèles*, UIT-T X.509, *L'annuaire: cadre général des certificats de clé publique et d'attribut* et UIT-T X.519, *L'annuaire: spécification des protocoles*, fournit des services d'annuaire pour faciliter les communications et l'échange d'informations entre des entités, des personnes, des terminaux, des listes de distribution, etc. Les services d'annuaire classiques sont notamment les suivants: nommage, correspondance nom-adresse, établissement d'un lien entre les objets et leur emplacement. Mais l'annuaire joue aussi un rôle important dans la prise en charge des services de sécurité par la définition et la conservation de justificatifs d'authentification sous la forme de certificats de sécurité. En particulier, la série de Recommandations UIT-T X.500 porte sur deux aspects de la sécurité:

- la protection des informations d'annuaire, définie essentiellement dans les Rec. UIT-T X.501 et UIT-T X.509; et
- les principes de base de l'infrastructure de clé publique (PKI) et de l'infrastructure de gestion de privilège (PMI), définis dans la Rec. UIT-T X.509.

Dans le présent chapitre, on commence par examiner l'importance que revêt la sécurité de l'annuaire proprement dit et la nécessité de protéger les informations de l'annuaire. On s'intéresse ensuite au rôle de l'annuaire dans la prise en charge de l'authentification forte, des infrastructures de clé publique, de la gestion d'identité et de la télébiométrie.

6.1 Protection des informations de l'annuaire

6.1.1 Objectifs de protection de l'annuaire

La protection des données, qui est un aspect important de la gestion d'identité, est constamment prise en compte dans les travaux relatifs à l'annuaire. La protection des données de l'annuaire est essentiellement une question de respect de la vie privée (à savoir éviter la divulgation non autorisée d'informations personnelles sensibles), mais elle implique également de garantir l'intégrité des données et de protéger les actifs représentés par les données.

Un annuaire contient des informations sur des entités. Ces informations peuvent être sensibles et ne devraient être communiquées qu'à ceux qui ont le droit de les obtenir et qui ont *besoin de savoir*.

On distingue trois aspects de la protection des données:

- authentification de l'utilisateur cherchant à accéder aux informations;
- contrôle d'accès afin de protéger les données contre tout accès non autorisé (NOTE – Une authentification correcte est nécessaire pour le contrôle d'accès); et
- protection de la confidentialité des données, pour laquelle un contrôle d'accès correct est nécessaire.

Presque dès le début, les caractéristiques de protection des données ont constitué une partie importante de la Rec. UIT-T X.500. La Rec. UIT-T X.500 est la seule spécification d'annuaire à décrire ces caractéristiques importantes.

6.1.2 Authentification des utilisateurs de l'annuaire

Un annuaire UIT-T X.500 peut autoriser l'accès anonyme à certaines de ses informations non sensibles. Cependant, pour pouvoir accéder à des données plus sensibles, un certain niveau d'authentification des utilisateurs est nécessaire. Dans la Rec. UIT-T X.500, plusieurs niveaux d'authentification sont définis:

- a) nom uniquement;
- b) nom et mot de passe non protégé (autrement dit le nom et un mot de passe qui est transmis en clair);
- c) nom et mot de passe protégé (autrement dit un mot de passe qui est haché avec d'autres informations afin de pouvoir détecter toute tentative d'accès à l'annuaire en réutilisant la même valeur de hachage); et
- d) authentification forte, pour laquelle l'expéditeur signe numériquement certaines informations. Les informations signées comprennent le nom du destinataire et d'autres informations qui permettent aussi de détecter toute tentative de réutilisation.

Le niveau requis de protection des données est différent suivant le type d'utilisateur qui cherche à accéder aux données. Le niveau d'authentification d'un utilisateur a également une incidence sur les droits d'accès de cet utilisateur.

6.1.3 Contrôle d'accès à l'annuaire

Le contrôle d'accès est utilisé pour permettre ou refuser des opérations sur certaines informations de l'annuaire. La Rec. UIT-T X.500 est très souple quant à la question de savoir comment subdiviser les informations d'annuaire et les utilisateurs aux fins du contrôle d'accès. Une information à protéger est appelée élément protégé. Les éléments protégés pour lesquels les propriétés de contrôle d'accès sont communes peuvent être regroupés. De même, les utilisateurs peuvent être regroupés en fonction des permissions ou des refus d'accès.

Les droits d'accès d'un utilisateur ou d'un groupe d'utilisateurs dépendent du niveau d'authentification. Le niveau d'authentification requis pour consulter des informations sensibles ou pour mettre à jour des entrées sera en principe plus élevé que celui qui est requis pour consulter des informations moins sensibles.

Le contrôle d'accès tient compte également du type d'accès aux données, par exemple lecture, adjonction, suppression, mise à jour et changement de noms. Dans certains cas, il se peut que les utilisateurs ne soient même pas au courant de l'existence de certaines informations.

Le contrôle d'accès se rapporte au droit de savoir mais dépend du besoin de savoir. Avoir le *droit de savoir* ne permet pas à un utilisateur de consulter des informations si le *besoin de savoir* n'est pas établi. Si le *besoin de savoir* n'est pas établi, la divulgation d'informations pourrait constituer une violation du respect de la vie privée.

Il existe plusieurs exemples dans lesquels le *droit de savoir* ne suffit pas, par exemple:

- même si un utilisateur a le droit de consulter les adresses postales individuelles de certaines entités, il peut être inopportun de permettre la consultation d'un grand nombre d'adresses postales;
- si un utilisateur possède des droits d'accès à certaines informations, ces droits ne s'appliquent peut-être pas à l'application particulière pour laquelle la consultation est réalisée, auquel cas il n'existe pas de *besoin de savoir* et les informations ne devraient pas être communiquées.

6.1.4 Protection de la confidentialité

La protection de la confidentialité des données UIT-T X.500 est unique et très puissante. Elle intervient principalement lorsqu'un utilisateur fait une recherche dans l'annuaire en fournissant des critères de recherche généraux qui pourraient donner un très grand nombre de résultats. (On parle parfois de pêche aux informations.)

La Rec. UIT-T X.500 utilise un concept d'administration de service reposant sur des tables qui, en plus de l'administration des services généraux, permet aussi d'assurer une protection de la confidentialité des données. L'administrateur crée une ou plusieurs tables pour chaque combinaison de type de service et de groupe d'utilisateurs. Pour que la consultation de données aboutisse, il faut avoir une table qui corresponde exactement au type de service et au type de groupe d'utilisateurs. Toutefois, cela ne suffit pas. La table est protégée par le contrôle d'accès, autrement dit l'utilisateur doit aussi avoir la permission d'accéder à la table en question.

Une table, également appelée règle de recherche, peut contenir des informations telles que:

- les critères de recherche requis, afin de cibler la recherche pour qu'elle donne un seul ou très peu de résultats, ce qui permet d'éviter que des recherches donnent de très nombreux résultats et d'assurer une protection contre la pêche aux données;
- une liste d'informations se rapportant au type de service; et
- des informations de contrôle des différentes entités représentées dans l'annuaire. La table utilisée interagit avec les informations de contrôle d'une entité afin de restreindre les informations renvoyées concernant cette entité. Cela permet d'adapter les données en fonction des critères de protection de la confidentialité pour chaque entité particulière. Les entités peuvent avoir des exigences spéciales, elles peuvent par exemple exiger que leur adresse postale ne soit pas divulguée et éventuellement qu'une fausse adresse soit renvoyée à la place ou encore que leur adresse de courrier électronique ne soit pas communiquée à certains groupes d'utilisateurs.

La protection des informations personnelles sensibles est importante pour plusieurs raisons. Plusieurs normes sur la sécurité, notamment celles qui ont trait à l'authentification des individus et à la gestion d'identité, reposent sur la collecte et le stockage d'informations d'identification personnelle sensibles. Dans un nombre croissant de juridictions, il existe des dispositions légales relatives à la collecte et à l'utilisation de ces informations. Les services et mécanismes de sécurité, qui sont nombreux à être fondés sur des normes de l'UIT-T, servent à protéger les informations qui sont sensibles du point de vue du respect de la vie privée. Le respect de la vie privée est abordé dans un certain nombre de Recommandations, dont certaines examinent directement l'impact de certaines technologies sur le respect de la vie privée. On peut citer par exemple la Recommandation UIT-T X.1171, *Menaces et protection requise pour les informations d'identification personnelle dans les applications utilisant l'identification par étiquette*, qui a été approuvée récemment et qui est examinée plus en détail dans le paragraphe 9.5 (Services par étiquette), et les lignes directrices sur la protection des informations d'identification personnelle dans les applications RFID, qui sont en cours d'élaboration par la Commission d'études 17 dans le cadre des travaux sur la gestion d'identité (voir paragraphe 6.4).

6.2 Authentification forte: mécanismes de sécurité à clé publique

Une infrastructure de clé publique (PKI, *public key infrastructure*) facilite la gestion des clés publiques pour assurer les services d'authentification, de chiffrement, d'intégrité et de non-répudiation. La technologie fondamentale de l'infrastructure PKI est la cryptographie à clé publique, qui est décrite ci-après. La Recommandation UIT-T X.509, *L'annuaire: cadre général des certificats de clé publique et d'attribut* est une norme PKI d'authentification forte fondée sur des certificats de clé publique et des autorités de certification. En plus de la définition d'un cadre d'authentification pour l'infrastructure PKI, la Rec. UIT-T X.509 définit aussi une infrastructure de gestion de privilège (PMI, *privilege management infrastructure*), qui sert à vérifier les droits et privilèges des utilisateurs dans le contexte d'une autorisation forte, fondée sur des certificats d'attribut et des autorités d'attribut. Les composants des infrastructures PKI et PMI sont illustrés sur la Figure 10.

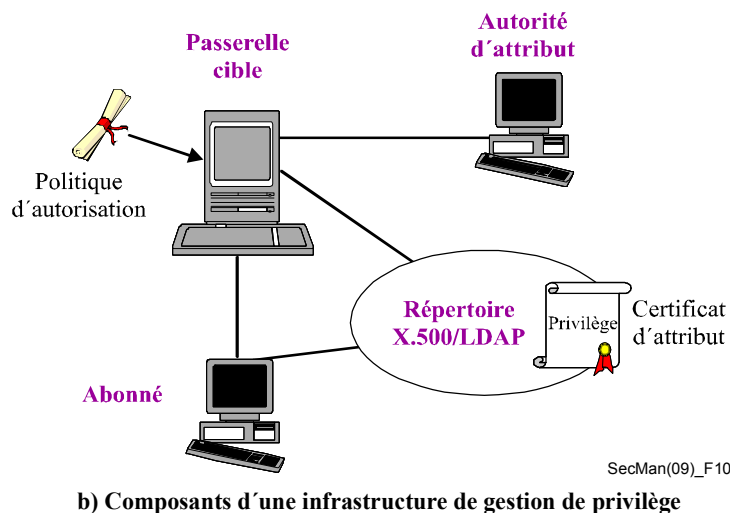
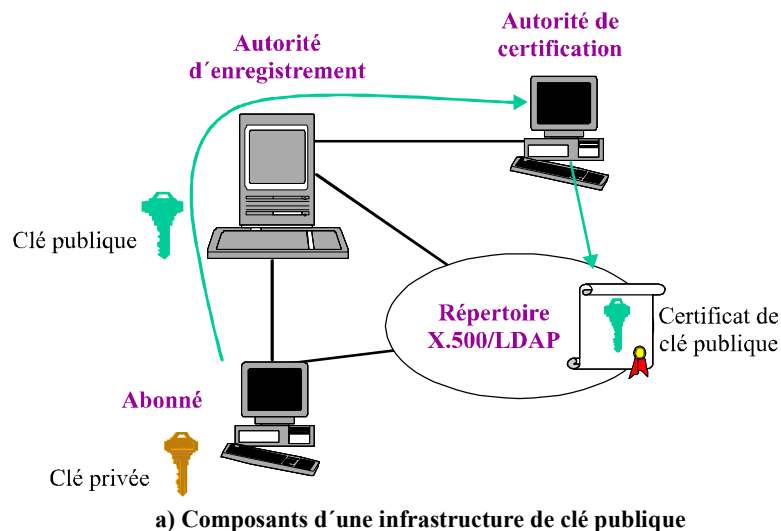


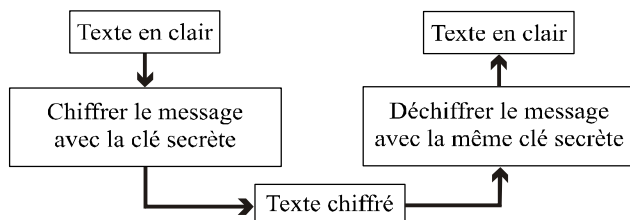
Figure 10 – Composants des infrastructures PKI et PMI

6.2.1 Cryptographie à clé secrète et cryptographie à clé publique

Dans un système de cryptographie *symétrique* (ou à *clé secrète*), on utilise la même clé pour le chiffrement et pour le déchiffrement, comme illustré sur la Figure 11 (a). Les individus en communication partagent donc une clé secrète unique. La clé doit être distribuée aux individus par des moyens sécurisés, car la connaissance de la clé de chiffrement implique la connaissance de la clé de déchiffrement et inversement.

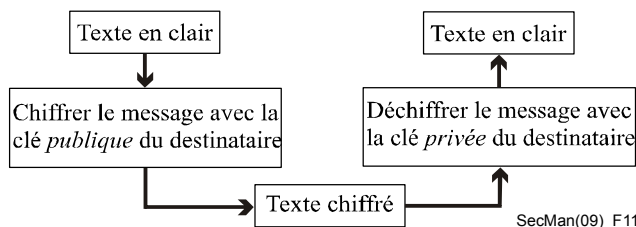
Un système de cryptographie *asymétrique* (ou à *clé publique*) fait intervenir deux clés, une clé publique et une clé privée, comme illustré sur la Figure 11 (b). La clé publique peut être distribuée largement alors que la clé privée doit toujours être gardée secrète. La clé privée est généralement conservée sur une carte à puce ou sur un jeton. La clé publique est produite à partir de la clé privée et, bien que ces clés soient liées mathématiquement, il est impossible d'inverser le processus afin de déduire la clé privée de la clé publique. Pour envoyer à un destinataire des données confidentielles en toute sécurité en utilisant le chiffrement à clé publique, l'expéditeur chiffre les données avec la clé publique du destinataire et le destinataire les déchiffre avec sa clé privée correspondante. On peut aussi utiliser le chiffrement à clé publique pour appliquer une signature numérique à des données, le but étant de fournir la confirmation qu'un document ou un message provient bien de la personne qui déclare être l'expéditeur (ou l'auteur). La signature numérique est en réalité

un condensé des données qui est produit au moyen de la clé privée du signataire et ajouté au document ou au message. Le destinataire utilise la clé publique du signataire pour confirmer la validité de la signature numérique. (NOTE – Certains systèmes à clé publique utilisent deux paires distinctes de clés publique/privée, l'une pour le chiffrement/déchiffrement, l'autre pour l'établissement/vérification de la signature numérique.)



- Les deux parties partagent une même clé secrète
- Problème: il est difficile d'échanger des clés dans un secret complet et ce type de chiffrement est difficilement applicable à une large communauté d'utilisateurs
- Exemple le plus connu: DES (norme de chiffrement des données)

a) Chiffrement à clé secrète (symétrique)



- Chaque participant a:
 - une clé privée qu'il ne partage avec personne d'autre
 - une clé publique que tout le monde connaît
- Problème: plus lent que le chiffrement à clé secrète
- Exemple le plus connu: RSA

b) Chiffrement à clé publique (asymétrique)

Figure 11 – Illustration des processus de chiffrement à clé secrète et à clé publique

Avec le chiffrement symétrique, chaque paire d'utilisateurs doit avoir des clés différentes et ces clés doivent être distribuées et conservées en toute sécurité. En revanche, avec le chiffrement asymétrique, les clés de chiffrement publiques peuvent être publiées dans l'annuaire et chacun peut utiliser la même clé de chiffrement (publique) pour envoyer des données à un utilisateur donné de façon sécurisée. Ainsi, le chiffrement asymétrique est beaucoup plus facilement applicable à une large communauté que le chiffrement symétrique. Toutefois, le chiffrement asymétrique nécessite de très longs calculs, de sorte qu'il est inefficace de chiffrer des messages entiers au moyen du chiffrement asymétrique. Dans la pratique, le chiffrement asymétrique est généralement utilisé pour distribuer des clés de chiffrement symétriques de façon sécurisée. Les clés symétriques sont ensuite utilisées pour chiffrer le corps du message au moyen d'un algorithme symétrique plus efficace sur le plan des calculs. Lorsqu'une signature numérique est requise, un condensé (ou une valeur de hachage) du message est produit au moyen d'une fonction de hachage unidirectionnelle sécurisée telle que SHA-1 ou MD5. La valeur de hachage est ensuite chiffrée (au moyen de la clé privée de l'expéditeur) puis jointe au message. Le destinataire peut confirmer la validité de la signature numérique en déchiffrant la signature numérique au moyen de la clé publique de l'expéditeur pour obtenir la valeur de hachage générée par l'expéditeur puis en créant sa propre valeur de hachage du message reçu. Les deux valeurs de hachage doivent être identiques pour que la signature soit valable.

Quel que soit le mode de chiffrement (symétrique ou asymétrique) utilisé, il est impossible d'acheminer des messages entièrement chiffrés (y compris les en-têtes) à leurs destinataires car les nœuds intermédiaires ne pourraient pas déterminer l'adresse du destinataire. Par conséquent, les en-têtes de message ne doivent généralement pas être chiffrés.

La sécurité de fonctionnement d'un système à clé publique dépend fortement de la validité des clés publiques. Les clés publiques sont normalement publiées sous la forme de certificats numériques qui sont conservés dans un annuaire UIT-T X.500. Un certificat contient non seulement la clé de chiffrement publique et, le cas échéant, la clé de vérification de la signature pour un individu, mais aussi d'autres informations, dont la validité du certificat. En principe, les certificats qui ont été révoqués pour une raison ou pour une autre sont aussi inscrits sur une liste de révocation de certificats (CRL, *certificate revocation list*) figurant dans l'annuaire. Avant d'utiliser des clés publiques, on vérifie normalement la liste CRL pour s'assurer de leur validité.

6.2.2 Certificats de clé publique

Un certificat de clé publique (parfois appelé "certificat numérique") est un moyen permettant de valider le propriétaire d'une paire de clés asymétriques. Un certificat de clé publique rattache fortement une clé publique à son propriétaire et il est signé numériquement par une autorité de confiance attestant ce rattachement. Cette autorité de confiance est appelée autorité de certification (CA, *certification authority*). Le format normalisé admis sur le plan international pour les certificats de clé publique est défini dans la Rec. UIT-T X.509. Un certificat de clé publique UIT-T X.509 comprend une clé publique, un identificateur de l'algorithme asymétrique avec lequel la clé doit être utilisée, le nom du propriétaire de la paire de clés, le nom de l'autorité de certification attestant cette propriété, le numéro de série et la période de validité du certificat, le numéro de la version UIT-T X.509 à laquelle ce certificat est conforme et un ensemble facultatif de champs d'extension contenant des informations sur la politique de certification de l'autorité de certification. Le certificat entier est signé numériquement au moyen de la clé privée de l'autorité de certification. Un certificat UIT-T X.509 peut être publié largement, par exemple sur un site web, dans un annuaire LDAP ou sur une carte de visite électronique (Vcard¹) jointe à des courriers électroniques. La signature de l'autorité de certification garantit que le contenu du certificat ne peut pas être modifié sans que cela ne soit détecté.

Pour confirmer la validité d'un certificat, l'utilisateur a besoin de pouvoir accéder à la clé publique valable de l'autorité de certification qui a émis ce certificat, afin de vérifier la signature de l'autorité de certification sur ce certificat. Étant donné que la clé publique d'une autorité de certification peut être certifiée par une autre autorité de certification (supérieure), la validation des clés publiques peut alors faire intervenir une chaîne de certificats et d'autorités de certification. Au bout du compte, cette chaîne doit avoir une fin, qui correspond généralement au certificat de l'autorité de certification qui constitue la "racine de confiance". Les clés publiques d'autorité de certification racine sont distribuées sous la forme de certificats autosignés (dans lesquels les autorités de certification racines attestent qu'il s'agit de leur propre clé publique). La signature permet alors à un utilisateur de confirmer que la clé et le nom de l'autorité de certification n'ont pas été altérés depuis la création du certificat. Toutefois, le nom de l'autorité de certification figurant dans un certificat autosigné ne peut pas être automatiquement considéré comme étant correct, car c'est l'autorité de certification qui a inséré le nom dans le certificat. Il est donc essentiel dans une infrastructure de clé publique que les clés publiques d'autorité de certification racine soient distribuées de manière sécurisée, afin de garantir qu'une clé publique appartient réellement à l'autorité de certification racine dont le nom figure dans le certificat autosigné. Sans cette garantie, l'utilisateur ne peut pas être sûr que l'identité de l'autorité de certification racine n'est pas usurpée.

¹ Une vCard est une carte de visite électronique de format standard qui est souvent échangée par courrier électronique.

6.2.3 Infrastructures de clé publique

L'infrastructure PKI est principalement destinée à émettre et gérer les certificats de clé publique, y compris les certificats d'autorité de certification racine. La gestion de clés comprend la création de paires de clés, la création de certificats de clé publique, la révocation de certificats de clé publique (par exemple si la clé privée d'un utilisateur a été compromise), le stockage et l'archivage des clés et des certificats et leur destruction une fois qu'ils sont arrivés au terme de leur vie. Chaque autorité de certification suit un ensemble de politiques. La Rec. UIT-T X.509 définit des mécanismes permettant de distribuer certaines de ces informations de politique dans les champs d'extension des certificats UIT-T X.509 émis par les autorités de certification. Les règles et procédures politiques suivies par une autorité de certification sont généralement définies dans une politique de certificat (CP, *certificate policy*) et dans une déclaration de pratique de certification (CPS, *certification practice statement*), qui sont des documents publiés par l'autorité de certification. Ces documents constituent une base commune permettant d'évaluer la confiance que l'on peut avoir concernant les certificats émis par les autorités de certification, à la fois sur le plan international et d'un secteur à l'autre. Ils constituent aussi une partie du cadre juridique nécessaire à l'établissement d'une confiance interorganisations et à la spécification de restrictions quant à l'utilisation des certificats émis.

Les premières versions de la Rec. UIT-T X.509 (1988, 1993 et 1997) spécifiaient les éléments de base nécessaires pour les infrastructures de clé publique et définissaient notamment les certificats de clé publique. La Rec. UIT-T X.509 révisée qui a été approuvée en 2001 (et mise à jour en 2005 et 2008) contient des précisions sur les certificats d'attribut et définit un cadre pour l'infrastructure de gestion de privilège (PMI, *privilege management infrastructure*).

6.2.4 Infrastructure de gestion de privilège

Une infrastructure de gestion de privilège (PMI) gère les privilèges pour prendre en charge un service d'autorisation complet en relation avec une infrastructure PKI. Les mécanismes définis permettent d'établir des privilèges d'accès pour les utilisateurs dans un environnement multifabricant et multi-application. Les infrastructures PMI et PKI utilisent des concepts analogues, mais l'infrastructure PMI concerne l'autorisation tandis que l'infrastructure PKI concerne l'authentification. Le Tableau 4 illustre les analogies entre les deux infrastructures.

Tableau 4 – Comparaison des caractéristiques de l'infrastructure de gestion de privilège et de l'infrastructure de clé publique

Infrastructure de gestion de privilège	Infrastructure de clé publique
Source d'autorité (SoA)	Autorité de certification racine (point d'ancrage de confiance)
Autorité d'attribut	Autorité de certification
Certificat d'attribut	Certificat de clé publique
Liste de révocation de certificats d'attribut	Liste de révocation de certificats
Liste de révocation d'autorités pour l'infrastructure PMI	Liste de révocation d'autorités pour l'infrastructure PKI

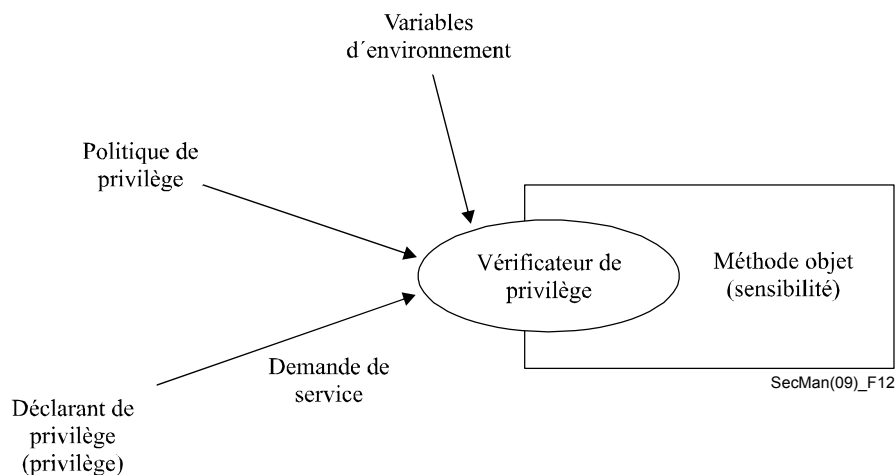
L'attribution de privilèges aux utilisateurs vise à faire en sorte que les utilisateurs suivent une politique de sécurité prescrite établie par la source d'autorité. Les informations relatives à la politique sont rattachées au nom d'utilisateur dans le certificat d'attribut et comprennent un certain nombre d'éléments illustrés dans le Tableau 5.

Tableau 5 – Structure d'un certificat d'attribut X.509

Version
Détenteur
Emetteur
Signature (identificateur d'algorithme)
Numéro de série de certificat
Durée de validité
Attributs
Identificateur unique de l'émetteur
Extensions

Les certificats d'attribut sont également utilisés en télébiométrie (voir le paragraphe 6.5) afin de créer des certificats biométriques pour rattacher un utilisateur à ses informations biométriques. Les certificats de dispositif biométrique définissent les capacités et les limitations des dispositifs biométriques. Les certificats de politique biométrique définissent la relation entre un niveau de sécurité et des paramètres d'algorithme biométrique.

Cinq composants sont décrits dans la Rec. UIT-T X.509 pour le contrôle de l'infrastructure PMI: le déclarant de privilège, le vérificateur de privilège, la méthode objet, la politique de privilège et les variables d'environnement (voir la Figure 12). Le vérificateur de privilège peut contrôler l'accès du déclarant de privilège à la méthode objet, conformément à la politique de privilège.

**Figure 12 – Modèle de contrôle de l'infrastructure PMI X.509**

Pour certaines implémentations, il peut être nécessaire de déléguer un privilège. Quatre composants sont pris en considération dans la Rec. UIT-T X.509 pour le modèle de délégation pour l'architecture PMI: le vérificateur de privilège, la source d'autorité, d'autres autorités d'attribut et le déclarant de privilège (voir la Figure 13).

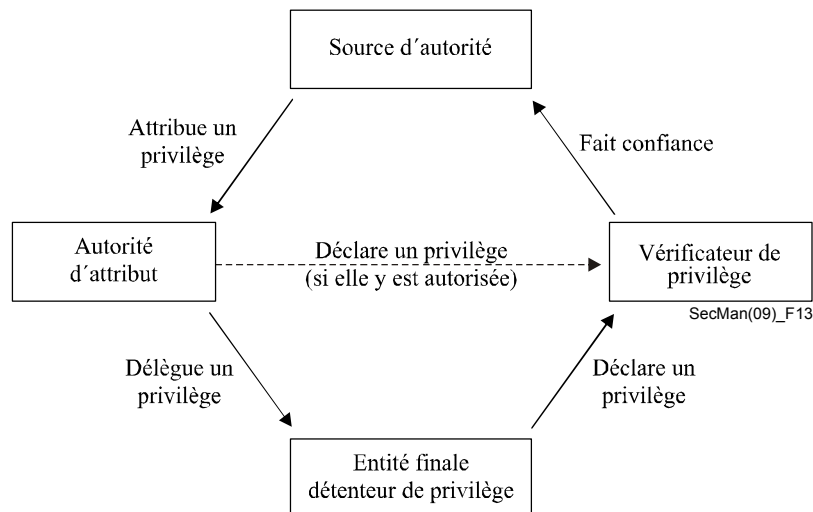


Figure 13 – Modèle de délégation pour l'infrastructure PMI X.509

Dans les implémentations récentes de systèmes d'autorisation fondées sur le modèle du contrôle d'accès basé sur le rôle (RBAC, *role-based access control*), on considère qu'un rôle est attribué à l'utilisateur. La politique d'autorisation associe un ensemble de permissions à un rôle. Lorsque l'utilisateur accède à une ressource, son rôle est d'abord vérifié avant qu'il ne puisse invoquer des actions.

6.3 Lignes directrices relatives à l'authentification

Un certain nombre de lignes directrices portant sur des aspects spécifiques de l'authentification ont été élaborées. Elles sont récapitulées ci-dessous.

6.3.1 Protocole d'authentification sûre fondée sur un mot de passe avec échange de clés

Le protocole d'authentification sûre fondée sur un mot de passe avec échange de clés (SPAK, *secure password-based authentication protocol with key exchange*) est un protocole d'authentification simple dans lequel l'utilisation d'un mot de passe facilement mémorisable entre un client et un serveur permet de procéder à une authentification mutuelle et d'utiliser un secret partagé comme clés de session pour la session suivante.

Les spécifications du protocole SPAK et les lignes directrices permettant de choisir celui qui convient le mieux parmi divers protocoles d'authentification sûre fondée sur un mot de passe sont définies dans la Rec. UIT-T X.1151, *Lignes directrices applicables à un protocole d'authentification sûre fondée sur un mot de passe avec échange de clés*. Ce protocole est très simple. Il est facile à mettre en œuvre et à utiliser et ne nécessite pas d'autre infrastructure (telle que PKI). Il devrait gagner en importance pour de nombreuses applications dans un avenir proche. Le protocole SPAK permet à la fois une authentification de l'utilisateur et un échange de clés avec un simple mot de passe. Une session de communication à venir peut ainsi être protégée par un secret qui est partagé pendant la procédure d'authentification (voir la Figure 14).

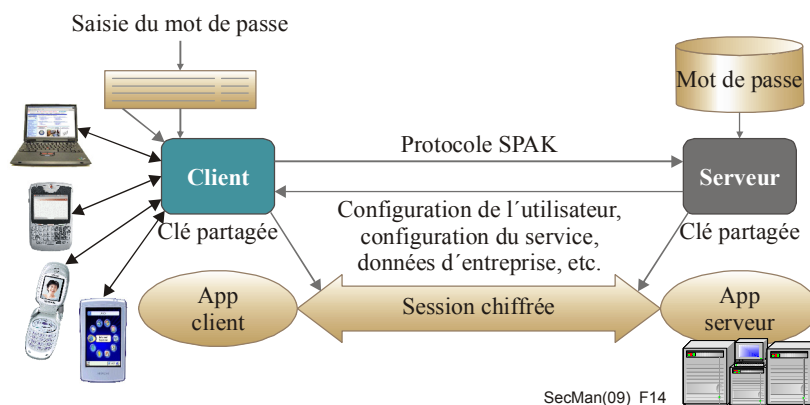


Figure 14 – Fonctionnement type du protocole SPAK

6.3.2 Protocole d'authentification extensible

Le protocole d'authentification extensible (EAP, *extensible authentication protocol*) prend en charge plusieurs mécanismes d'authentification entre un suppliant et un serveur d'authentification dans un réseau de communication de données. Le protocole EAP peut servir d'outil de base pour l'activation de l'authentification de l'utilisateur et la distribution des clés de session. Il peut permettre d'authentifier un dispositif afin d'établir une connexion point à point sécurisée et d'interdire l'accès aux dispositifs non autorisés.

La Recommandation UIT-T X.1034 décrit un cadre applicable à l'authentification et à la gestion de clé basées sur le protocole EAP pour sécuriser les couches inférieures dans un réseau de communication. Elle donne des indications sur le choix des méthodes EAP et décrit le mécanisme de gestion de clé pour les couches inférieures d'un réseau de communication de données. Le cadre s'applique à la fois aux réseaux d'accès sans fil et aux réseaux d'accès filaires avec un support partagé.

Trois entités sont nécessaires pour l'authentification et la gestion de clé: un suppliant (ou homologue), un authentificateur et un serveur d'authentification, comme indiqué sur la Figure 15. Le suppliant fonctionne comme un utilisateur final, qui accède au réseau depuis une station d'utilisateur final. L'authentificateur joue le rôle d'entité d'application de politiques, qui relaie les messages EAP entre le suppliant et le serveur d'authentification. Le serveur d'authentification authentifie le suppliant, partage facultativement un secret qui peut être utilisé pour déduire des clés cryptographiques, envoie le résultat de l'authentification d'un utilisateur final à l'authentificateur, et retransmet le secret partagé à l'authentificateur. Ce secret partagé peut servir à déduire des clés cryptographiques entre l'authentificateur et le suppliant pour garantir la confidentialité et l'intégrité et permettre l'authentification des messages.

L'authentification et la gestion de clé comprennent généralement quatre phases: découverte des capacités de sécurité, authentification EAP, distribution de clé, gestion de clé (voir la Figure 15). Dans la phase relative aux capacités de sécurité, le suppliant négocie les capacités de sécurité et les divers paramètres du protocole à utiliser avec l'authentificateur. Dans la phase EAP, le serveur d'authentification authentifie le suppliant et déduit un secret principal partagé avec le suppliant comme résultat du protocole EAP. Dans la phase de distribution de clé, le serveur d'authentification transmet le secret principal à l'authentificateur pour permettre de déduire diverses clés cryptographiques pour une session à venir entre le suppliant et l'authentificateur. Pour éviter de réutiliser sans cesse la même clé secrète, il convient d'utiliser de nouvelles clés cryptographiques dans chaque session. Enfin, dans la phase de gestion de clé, l'authentificateur échange des nombres aléatoires avec le suppliant pour obtenir une nouvelle clé cryptographique, conduisant à une confidentialité parfaite.

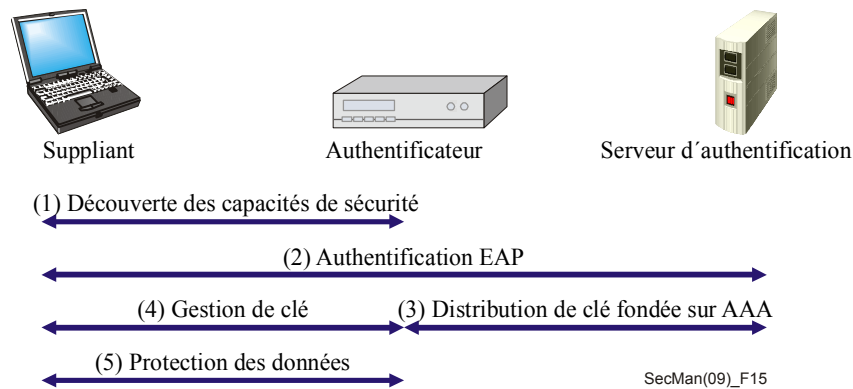


Figure 15 – Quatre phases pour l'authentification et la gestion de clé pour la couche inférieure

6.4 Gestion d'identité

6.4.1 Aperçu de la gestion d'identité

La gestion d'identité (IdM, *identity management*) consiste à gérer de façon sécurisée et à contrôler les informations d'identité (par exemple justificatifs, identificateurs, attributs et réputations) qui sont utilisées pour représenter les entités (fournisseurs de service, organisations d'utilisateurs finals, personnes, dispositifs de réseau, applications logicielles et services) dans le processus de communications. Une même entité peut avoir plusieurs identités numériques afin d'accéder à divers services avec différentes spécifications, ces identités pouvant exister à plusieurs endroits. L'IdM prend en charge l'authentification d'une entité. Aux fins de l'UIT-T, l'identité assertée par une entité représente l'unicité de cette entité dans un contexte donné.

L'IdM est essentielle pour la cybersécurité car elle permet d'établir et de maintenir des communications fiables entre les entités et permet un accès nomade à la demande aux réseaux et aux cyberservices. Elle permet aussi d'autoriser toute une gamme de privilèges (et non des privilèges tout ou rien) et facilite la modification des privilèges en cas de changement de rôle d'une entité. L'IdM permet à une organisation de mieux appliquer ses politiques de sécurité grâce à la possibilité de surveiller et de vérifier les activités d'une entité sur le réseau et permet à des entités de disposer d'un accès aussi bien à l'intérieur qu'à l'extérieur d'une organisation.

L'IdM permet de garantir des informations d'identité, avec un contrôle d'accès sécurisé. Cette capacité est offerte grâce à la connexion unique / déconnexion unique, au contrôle par l'utilisateur des informations d'identification personnelle et à la possibilité pour un utilisateur de choisir un fournisseur d'identité qui peut assurer des fonctions de vérification et de délégation pour son compte, par opposition à la fourniture de justificatifs à chaque fournisseur de service. L'IdM prend également en charge une multitude de services fondés sur l'identité: publicité ciblée, services personnalisés basés sur l'emplacement géographique et l'intérêt, services avec authentification pour diminuer la fraude et le vol d'identité, etc.

L'IdM est une technologie complexe qui inclut:

- l'établissement, la modification, la suspension, l'archivage et la suppression d'informations d'identité;
- la reconnaissance d'identités partielles qui représentent des entités dans un contexte ou un rôle spécifique;
- l'établissement et l'évaluation de la confiance entre des entités; et
- la localisation des informations d'identité d'une entité (par exemple via un fournisseur d'identité faisant autorité qui est légalement responsable de la conservation des identificateurs, des justificatifs et de tout ou partie des attributs de l'entité).

Le supplément à la série UIT-T X.1250, qui contient un aperçu de la gestion d'identité dans le contexte de la cybersécurité, présente brièvement ce qu'est la gestion d'identité.

6.4.2 Travaux de l'UIT-T sur la gestion d'identité

Même si des discussions sont toujours en cours sur certains concepts fondamentaux et sur un certain vocabulaire de base, les travaux progressent dans un certain nombre de domaines au sein de la CE 17 (qui est la Commission d'études directrice pour la gestion d'identité), de la CE 2 (aspects opérationnels de la fourniture de service et de la gestion des télécommunications) et de la CE 13 (réseaux futurs, y compris les réseaux mobiles et les réseaux de prochaine génération (NGN)).

La CE 2 mène des études se rapportant à la garantie de la cohérence du format et de la structure des identificateurs de gestion d'identité (IdM) et à la spécification des interfaces avec les systèmes de gestion afin de prendre en charge la communication des informations d'identité à l'intérieur d'un domaine organisationnel ou entre des domaines organisationnels.

La CE 13 mène des études se rapportant à une architecture fonctionnelle de gestion d'identité propre aux NGN qui prend en charge des services d'identité à valeur ajoutée, l'échange sécurisé d'informations d'identité et l'interopérabilité entre divers formats d'informations d'identité. Elle mène également des études se rapportant à la détermination des menaces liées à la gestion d'identité dans les NGN et des mécanismes de lutte contre ces menaces. La Recommandation UIT-T Y.2720, *Cadre de gestion d'identité dans les NGN*, a déjà été approuvée. Cette norme décrit une approche structurée pour concevoir, définir et mettre en œuvre des solutions IdM et faciliter l'interopérabilité dans des environnements hétérogènes.

La CE 17 est chargée d'étudier l'élaboration d'un modèle générique de gestion d'identité, indépendant des technologies de réseau et prenant en charge l'échange sécurisé d'informations d'identité entre des entités. Il s'agit aussi d'étudier le processus de découverte des sources d'informations d'identité qui font autorité, les mécanismes génériques pour l'interopérabilité de divers formats d'informations d'identité, les menaces liées à la gestion d'identité, les mécanismes de lutte contre ces menaces et la protection des informations d'identification personnelle (PII) et d'élaborer des mécanismes garantissant que l'accès aux informations PII n'est autorisé que lorsque cet accès est approprié. En septembre 2009, deux Recommandations ont été approuvées: la Rec. UIT-T X.1250, *Capacités de base pour l'amélioration de la confiance et de l'interopérabilité globales dans la gestion d'identité* et la Rec. UIT-T X.1251, *Cadre de contrôle de l'identité numérique par l'utilisateur*. Par ailleurs, un ensemble de définitions de base liées à la gestion d'identité (IdM) est en préparation pour faire en sorte que les normes de l'UIT-T sur la gestion d'identité emploient une terminologie uniforme et cohérente.

Une activité conjointe de coordination pour la gestion d'identité (JCA-IdM) a été établie pour coordonner les activités de l'UIT-T relatives à la gestion d'identité. Une initiative de normalisation mondiale de la gestion d'identité (IdM-GSI) a également été établie pour harmoniser les différentes approches relatives à la gestion d'identité dans le monde et pour collaborer avec d'autres organismes travaillant dans ce domaine. La page de la Commission d'études directrice pour la gestion d'identité contient de nombreuses informations sur les activités dans ce domaine, les Recommandations approuvées et les Recommandations en cours d'élaboration sur la gestion d'identité et d'autres informations sur les travaux relatifs à la gestion d'identité.

6.5 Télébiométrie

La télébiométrie vise à identifier et à authentifier les personnes au moyen de dispositifs biométriques dans des environnements de télécommunication. L'un des objectifs est d'améliorer l'identification et l'authentification des utilisateurs grâce à l'utilisation de méthodes télébiométriques sûres et sécurisées. Les travaux de l'UIT-T dans ce domaine sont menés en étroite coopération avec d'autres organisations de normalisation et portent notamment sur les aspects suivants: interaction entre un être humain et l'environnement, clés numériques biométriques, extensions biométriques des certificats X.509 et authentification biométrique dans un réseau ouvert.

6.5.1 Authentification télébiométrique

La biométrie permet d'offrir des services d'authentification hautement sécurisés, mais la normalisation de l'authentification biométrique sur un réseau ouvert fait face à un certain nombre de problèmes:

- il se peut que les fournisseurs de service ne soient pas informés des dispositifs biométriques qui sont utilisés dans l'environnement de l'utilisateur final, du niveau ou des paramètres de sécurité de ces dispositifs, ou de leur mode de fonctionnement;
- la précision (taux de fausses acceptations) déterminée par le paramètre de seuil varie en fonction des produits biométriques. Le fournisseur de service ne peut donc pas déclarer maintenir un niveau de précision uniforme; et
- la précision de la vérification biométrique peut baisser avec le vieillissement des utilisateurs finals, car la biométrie utilise des caractéristiques du corps humain.

Les protocoles généraux d'authentification biométrique et les profils pour les systèmes de télécommunication dans un réseau ouvert sont spécifiés dans la Recommandation UIT-T X.1084, *Protocole général d'authentification biométrique et profils types pour les systèmes de télécommunication*.

La Figure 16 illustre l'authentification d'un utilisateur final via un réseau ouvert sans contact direct.

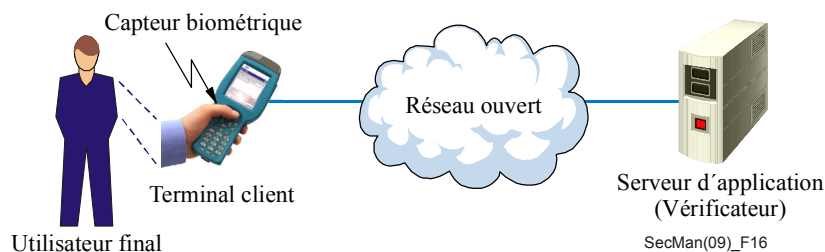


Figure 16 – Authentification télébiométrique d'un utilisateur final

6.5.2 Génération et protection des clés numériques télébiométriques

Un cadre pour la génération des clés numériques biométriques a été défini dans la Rec. UIT-T X.1088, *Cadre pour la génération et la protection des clés numériques biométriques*. Ce cadre définit la protection sur la base d'un modèle biométrique avec un certificat de clé publique et un certificat biométrique afin d'assurer une authentification sécurisée par le chiffrement et des communications sécurisées sur des réseaux ouverts. Des spécifications de sécurité sont également définies pour la génération et la protection des clés numériques biométriques. Le cadre peut être appliqué au chiffrement biométrique et à la signature numérique. Deux méthodes sont proposées:

- génération de clé biométrique, dans laquelle la clé est créée à partir d'un modèle biométrique (Figure 17); et
- liaison/rétablissement de clé biométrique, dans laquelle la clé est stockée dans une base de données et peut être extraite par authentification biométrique (Figure 18).

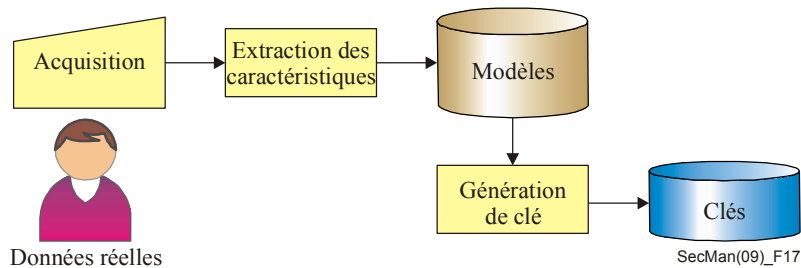


Figure 17 – Génération de clé biométrique

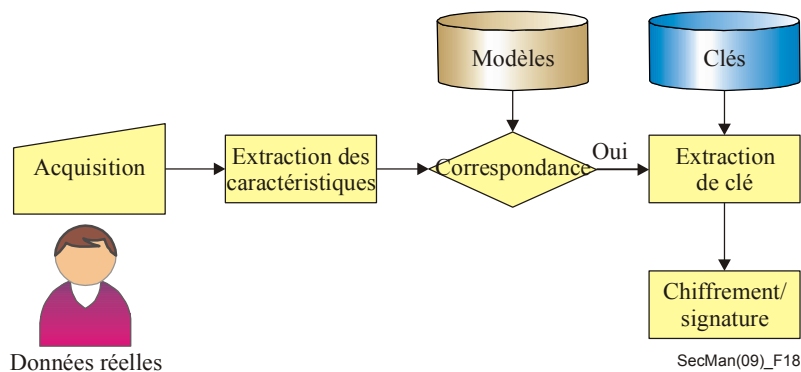


Figure 18 – Liaison/rétablissement de clé biométrique

6.5.3 Aspects de sécurité et de sûreté de la télébiométrie

Un cadre pour les aspects de sécurité et de sûreté de la télébiométrie a été défini dans le modèle multimodal télébiométrique (Rec. UIT-T X.1081, *Cadre général pour la spécification des aspects de sécurité et d'innocuité de la télébiométrie*), qui définit les interactions entre un être humain et l'environnement ainsi que les grandeurs et unités utilisées pour mesurer ces interactions. Le modèle multimodal télébiométrique ne se limite pas à la prise en compte des interactions purement physiques, mais il prend également en compte les interactions comportementales qui ne sont actuellement pas quantifiées par des unités standards.

6.5.4 Télébiométrie relative à la physiologie humaine

Les aspects de sécurité et de sûreté de la télébiométrie sont également pris en compte dans la Recommandation UIT-T X.1082, *Télébiométrie relative à la physiologie humaine*, qui définit des grandeurs et des unités pour les caractéristiques physiologiques, biologiques ou comportementales qui pourraient servir de données d'entrée ou de données de sortie pour des systèmes d'identification ou de vérification biométriques (systèmes de reconnaissance), y compris les seuils de détection ou de sécurité connus. Cette Recommandation donne des noms, des définitions et des symboles de grandeurs et d'unités pour la télébiométrie relative à la physiologie humaine (c'est-à-dire les caractéristiques humaines et les émissions qui peuvent être détectées par un capteur). Elle porte aussi sur des grandeurs et des unités relatives aux effets sur l'être humain causés par l'utilisation de dispositifs télébiométriques.

6.5.5 Autres éléments définis dans les normes sur la télébiométrie

Des extensions ont été définies pour les certificats UIT-T X.509 utilisés dans les infrastructures de clé publique ou dans les infrastructures de gestion de privilège afin de produire des certificats biométriques. Elles sont spécifiées dans la Rec. UIT-T X.1089, *Infrastructure d'authentification télébiométrique*.

La Recommandation UIT-T X.1083, *Protocole d'interfonctionnement à l'interface BioAPI* spécifie la syntaxe (utilisant l'ASN.1), la sémantique et le codage des messages qui permettent à une application conforme BioAPI de demander des opérations biométriques dans des fournisseurs de service biométrique conformes BioAPI (BSP) de part et d'autre des frontières entre des nœuds ou des processus, et de recevoir notification des événements provenant de ces BSP distants.

7. Sécurisation de l'infrastructure des réseaux

7 Sécurité de l'infrastructure des réseaux

Les données utilisées pour surveiller et contrôler le trafic de gestion des réseaux de télécommunication sont souvent transmises dans un réseau distinct qui achemine uniquement le trafic de gestion de réseau (pas le trafic des utilisateurs). Ce réseau, souvent appelé réseau de gestion des télécommunications (RGT), est décrit dans la Recommandation UIT-T M.3010, *Principes du réseau de gestion des télécommunications*. Il est impératif que ce trafic soit sécurisé. Le trafic de gestion est généralement classé dans différentes catégories en fonction des informations requises pour exécuter les fonctions de gestion des dérangements, de la configuration, de la qualité de fonctionnement, de la comptabilité et de la sécurité. La gestion de la sécurité de réseau concerne à la fois l'établissement d'un réseau de gestion sécurisé et la gestion de la sécurité des informations liées aux trois plans de sécurité de l'architecture de sécurité X.805.

L'activité de gestion des éléments d'infrastructure d'un réseau doit toujours être entreprise de manière sécurisée. Par exemple, les activités de réseau ne doivent être réalisées que par un utilisateur autorisé. Pour pouvoir offrir une solution sécurisée de bout en bout, des mesures de sécurité (par exemple contrôle d'accès, authentification) doivent être appliquées à chaque type d'activité de réseau concernant l'infrastructure du réseau, les services de réseau et les applications de réseau. Un certain nombre de Recommandations UIT-T portent tout particulièrement sur l'aspect de sécurité du plan de gestion en ce qui concerne les éléments de réseau et les systèmes de gestion qui font partie de l'infrastructure du réseau.

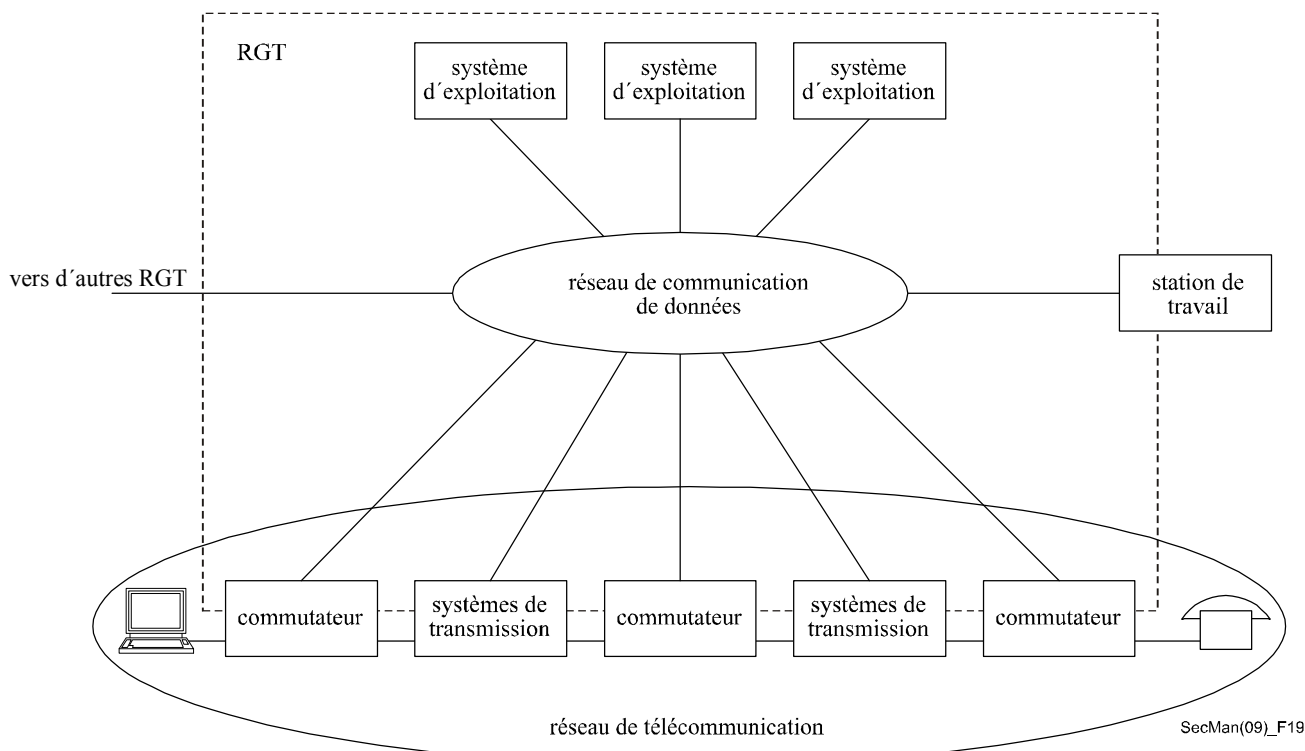
Parmi les autres applications de gestion de réseau, on peut citer celles qui se rapportent aux environnements dans lesquels différents fournisseurs de services doivent interagir pour offrir des services de bout en bout, par exemple dans le cas où des moyens de communication sont fournis à des organismes de réglementation ou à des organismes publics en vue d'assurer le retour à la normale après une catastrophe ou le cas où des lignes louées par des clients traversent des frontières géographiques.

7.1 Le réseau de gestion des télécommunications

Le RGT est séparé et isolé de l'infrastructure du réseau public de sorte que les perturbations dues à des menaces de sécurité dans le plan d'utilisateur final du réseau public ne s'étendent pas au RGT. Compte tenu de cette séparation, il est relativement facile de sécuriser le trafic du réseau de gestion car l'accès au plan de gestion est restreint aux administrateurs de réseau autorisés et le trafic est restreint aux activités de gestion valables. Avec la mise en place des réseaux de prochaine génération, le trafic des applications d'utilisateur final risque parfois d'être combiné au trafic de gestion. Cette approche, fondée sur une seule infrastructure de réseau intégrée, permet de minimaliser les coûts mais pose bon nombre de nouveaux problèmes de sécurité. Les menaces dans le plan d'utilisateur final constituent alors des menaces pour les plans de gestion et de commande car le plan de gestion devient maintenant accessible à une multitude d'utilisateurs finals et de nombreux types d'activités malveillantes deviennent possibles.

7.2 Architecture de gestion de réseau

L'architecture permettant de définir la gestion d'un réseau de télécommunication est définie dans la Rec. UIT-T M.3010. La relation entre un RGT et un réseau de télécommunication est illustrée sur la Figure 19. L'architecture du réseau de gestion définit des interfaces qui déterminent les échanges requis pour assurer les fonctions d'exploitation, d'administration, de maintenance et de configuration.



NOTE – La limite du RGT (ligne en pointillés) peut s'étendre jusqu'aux services et équipements de clients/utilisateurs et à leur gestion.

Figure 19 – Relation entre un RGT et un réseau de télécommunication

La Recommandation UIT-T M.3016.0 fournit un aperçu général et un cadre qui identifient les menaces de sécurité concernant un RGT. Dans la série UIT-T M.3016, la Rec. UIT-T M.3016.1 donne des détails sur les spécifications de sécurité, la Rec. UIT-T M.3016.2 décrit les services de sécurité et la Rec. UIT-T M.3016.3 définit des mécanismes permettant de faire face aux menaces dans le contexte de l'architecture fonctionnelle du RGT définie dans la Rec. UIT-T M.3010. Comme les spécifications n'ont pas besoin d'être toutes prises en charge par toutes les organisations, la Rec. M.3016.4 contient un formulaire permettant de créer des profils des spécifications, des services et des mécanismes de sécurité. Ce formulaire peut être utilisé pour assurer la conformité à la politique de sécurité propre à une organisation.

Lorsqu'on examine la gestion de la sécurité de réseau, deux facettes sont à prendre en considération. La première concerne le plan de gestion pour une activité de bout en bout entre utilisateurs (par exemple services de téléphonie IP). L'administration des utilisateurs doit être réalisée de manière sécurisée. On parle de *sécurité des informations de gestion* échangées sur le réseau pour la prise en charge d'une application de bout en bout. La deuxième facette est la *gestion des informations de sécurité*, qui s'applique quelle que soit l'application. Par exemple l'activité de signalisation de dérangement entre deux fournisseurs de services doit être réalisée en toute sécurité. Pour cela, un chiffrement des échanges peut être nécessaire, auquel cas il faut prévoir de gérer les clés de chiffrement.

Plusieurs Recommandations portant sur des fonctions de gestion de la sécurité de l'architecture X.805 sont disponibles pour les trois couches du plan de gestion (voir la Figure 1). De plus, comme on le verra dans les paragraphes qui suivent, d'autres Recommandations définissent des services génériques ou communs, par exemple l'envoi d'alarme en cas de violation de la sécurité, des fonctions d'audit et des modèles d'information qui définissent des niveaux de protection pour différentes cibles.

7.3 Sécurisation des éléments d'infrastructure d'un réseau

La connectivité de bout en bout peut être prise en considération en termes de réseaux d'accès et de réseaux centraux. Différentes technologies peuvent être employées dans ces réseaux. Des Recommandations ont été élaborées pour les deux types de réseau (réseau d'accès et réseau central). On prend ici l'exemple du réseau optique passif à large bande (BPON, *broadband passive optical network*). L'administration des privilèges des utilisateurs pour un tel réseau d'accès est définie au moyen de la méthodologie de modélisation unifiée définie dans la Rec. UIT-T Q.834.3. L'échange de gestion reposant sur l'architecture de courtier commun de requêtes d'objets (CORBA, *common object request broker architecture*) est spécifié dans la Rec. UIT-T Q.834.4. L'interface décrite dans ces Recommandations est appliquée entre le système de gestion des éléments et le système de gestion du réseau. Le système de gestion des éléments sert à gérer les différents éléments de réseau et a donc connaissance des détails internes des architectures matérielle et logicielle des éléments d'un ou de plusieurs fournisseurs et le système de gestion du réseau réalise les activités au niveau du réseau de bout en bout et couvre les systèmes de gestion de plusieurs fournisseurs. La Figure 20 montre les divers objets utilisés pour créer, supprimer, attribuer et utiliser des informations de contrôle d'accès pour les utilisateurs du système de gestion des éléments. La liste de permissions des utilisateurs contient la liste des activités de gestion qui sont permises pour chaque utilisateur autorisé. Le gestionnaire de contrôle d'accès vérifie l'identifiant et le mot de passe de l'utilisateur de l'activité de gestion et autorise l'accès en fonction de la fonctionnalité figurant dans la liste de permissions.

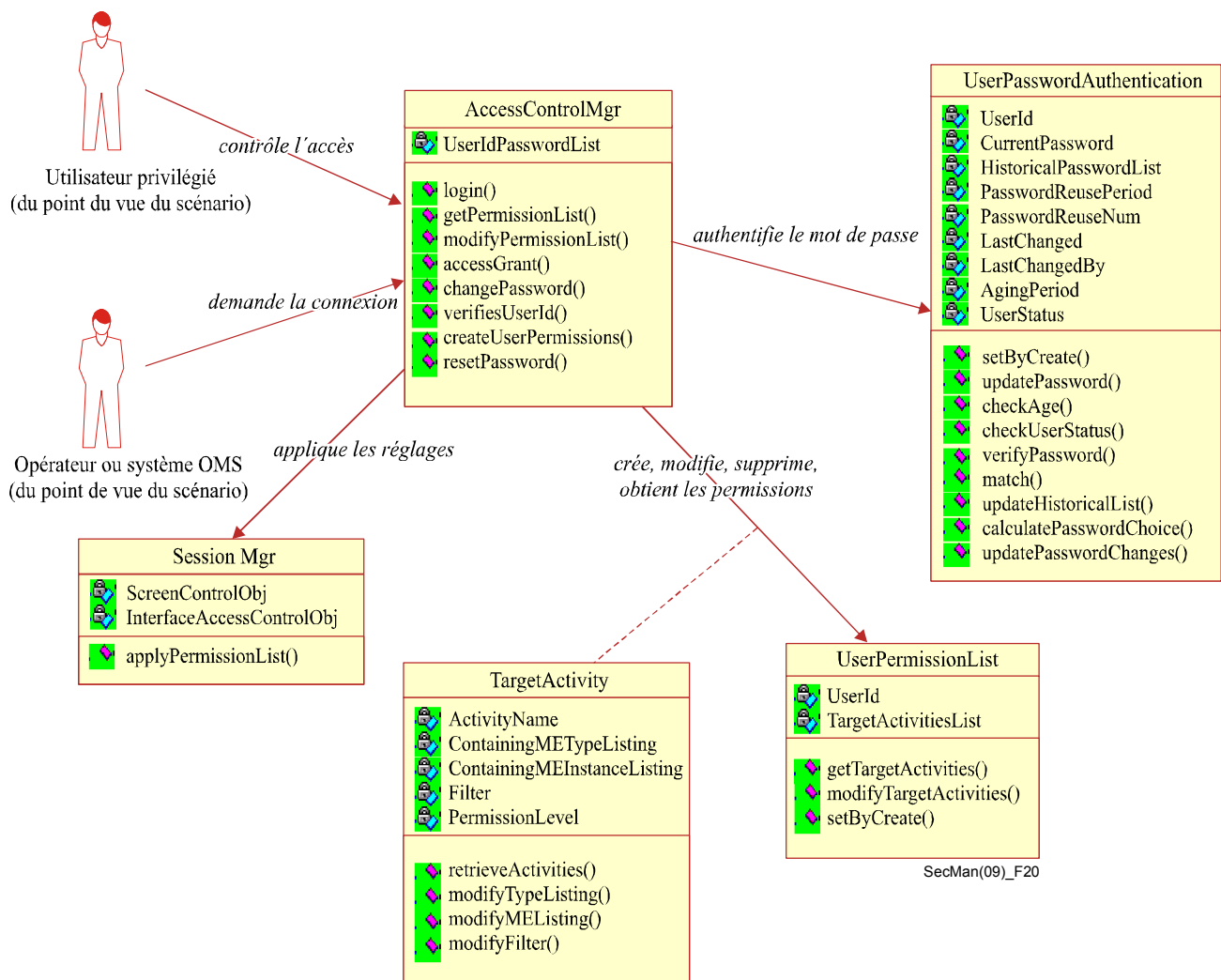


Figure 20 – Administration des privilèges des utilisateurs (UIT-T Q.834.3)

7.4 Sécurisation des activités de surveillance et de contrôle

Deux aspects de sécurité s'appliquent à l'intersection entre le plan de gestion et la couche services. Le premier aspect consiste à veiller à ce que des mesures de sécurité appropriées soient disponibles pour les services offerts dans le réseau (par exemple veiller à ce que seuls des utilisateurs valables soient autorisés à exécuter les opérations associées à la configuration d'un service). Le second aspect consiste à définir les échanges administratifs et de gestion qui sont valables afin de faciliter la détection des violations de sécurité.

La Recommandation UIT-T M.3208.2, *Gestion des connexions de liaison de service préapprouvonnées pour la formation d'un service de circuit loué*, porte sur le premier aspect, l'activité de gestion d'un service. Ce service de gestion de connexion permet à un abonné de créer/activer, modifier et supprimer des circuits loués dans les limites des ressources préconfigurées. Comme l'utilisateur configure la connectivité de bout en bout, il est nécessaire de garantir que seuls les utilisateurs autorisés peuvent exécuter ces opérations. Les dimensions de sécurité X.805 associées à ce service sont: l'authentification d'entité homologue, le contrôle d'intégrité des données (afin d'empêcher toute modification non autorisée des données en transit) et le contrôle d'accès (pour garantir qu'un abonné n'accède pas de façon malveillante ou accidentelle aux données d'un autre abonné).

La Recommandation UIT-T M.3210.1, *Services de gestion RGT pour la gestion de la sécurité des réseaux IMT-2000*, qui définit les activités administratives associées au plan de gestion pour les services hertziens, est un exemple de norme qui porte sur le second aspect. Dans un réseau hertzien, lorsque les utilisateurs se déplacent entre leur réseau de rattachement et un réseau visité, ils peuvent traverser différents domaines administratifs. Les services définis dans la Rec. UIT-T M.3210.1 décrivent comment le domaine de gestion des fraudes du réseau de rattachement collecte les informations appropriées concernant un abonné qui est enregistré dans un réseau visité. Les scénarios a) et b) de la Figure 21 illustrent le déclenchement de l'activité de gestion de surveillance respectivement par le réseau de rattachement et par le réseau visité. Le système de détection des fraudes du réseau de rattachement demande des informations sur les activités d'un abonné qui s'enregistre dans un réseau visité et reste actif jusqu'à ce que cet abonné annule son enregistrement dans ce réseau. Des profils d'utilisation peuvent alors être élaborés sur la base d'une analyse des relevés d'appel au niveau du service ou pour un abonné. Le système de détection des fraudes peut procéder à une analyse et produire des alarmes appropriées lorsqu'un comportement frauduleux est détecté.

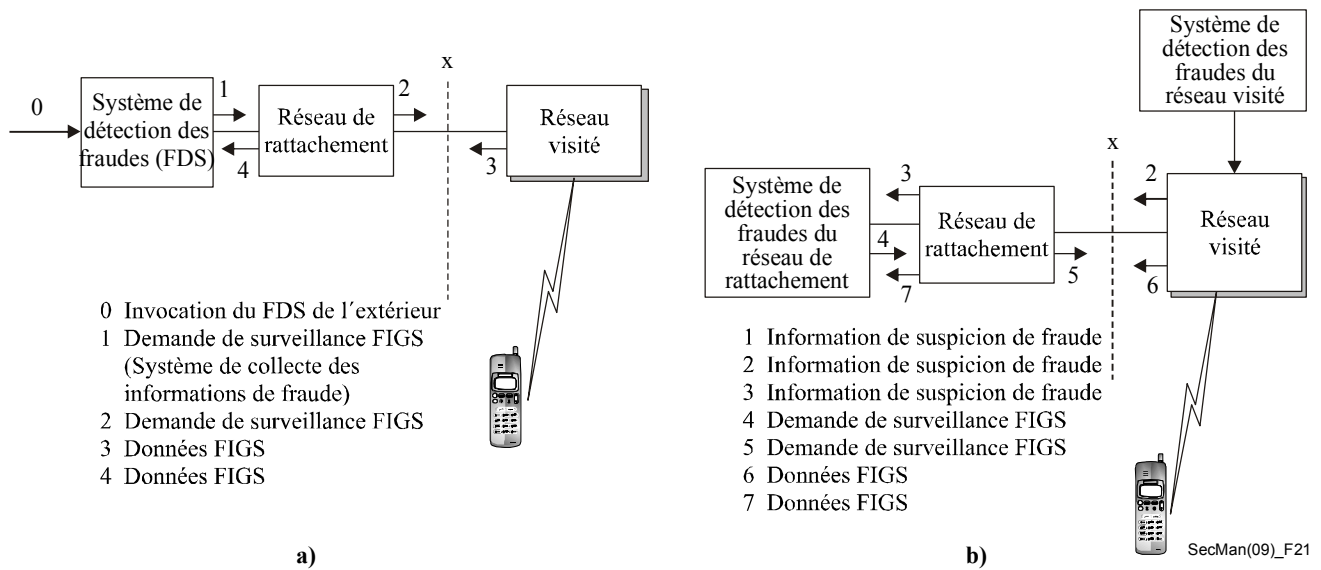


Figure 21 – Gestion des fraudes pour les services hertziens

7.5 Sécurisation des applications fondées sur le réseau

L'intersection du plan de gestion et de la couche application dans la Rec. UIT-T X.805 correspond à la sécurisation des applications d'utilisateur final fondées sur le réseau, par exemple la messagerie et l'annuaire. Une autre catégorie d'applications pour lesquelles les activités de gestion doivent être sécurisées est celle des applications de gestion proprement dites. La meilleure explication sera fournie au moyen d'exemples. Pour ces applications, le personnel de gestion (d'exploitation) du fournisseur de service représente les utilisateurs finals. Prenons le cas où un fournisseur de service utilise les services de connexion d'un autre fournisseur pour offrir un service de connectivité de bout en bout. Suivant l'environnement réglementaire ou le marché considéré, certains fournisseurs de services peuvent offrir des services d'accès et d'autres, appelés *opérateurs intercentraux*, peuvent offrir une connectivité longue distance. Les opérateurs intercentraux louent des services d'accès auprès du fournisseur local pour assurer la connectivité de bout en bout entre des endroits géographiques différents. En cas de perte de service, il est fait appel à une application appelée *administration des dossiers de dérangement* afin de signaler le problème. L'utilisateur de ces systèmes, ainsi que l'application proprement dite, a besoin d'une autorisation pour pouvoir signaler des problèmes. Les systèmes et utilisateurs autorisés doivent prendre les mesures qui s'imposent pour extraire l'état du ou des problèmes signalés. La Figure 22 illustre les interactions qui doivent être réalisées de manière sécurisée. Les privilèges d'accès sont administrés afin d'éviter tout accès non autorisé aux dossiers de dérangement. Un fournisseur de services est autorisé à signaler uniquement des dérangements concernant les services qu'il loue et non des dérangements concernant les services loués par un fournisseur différent.

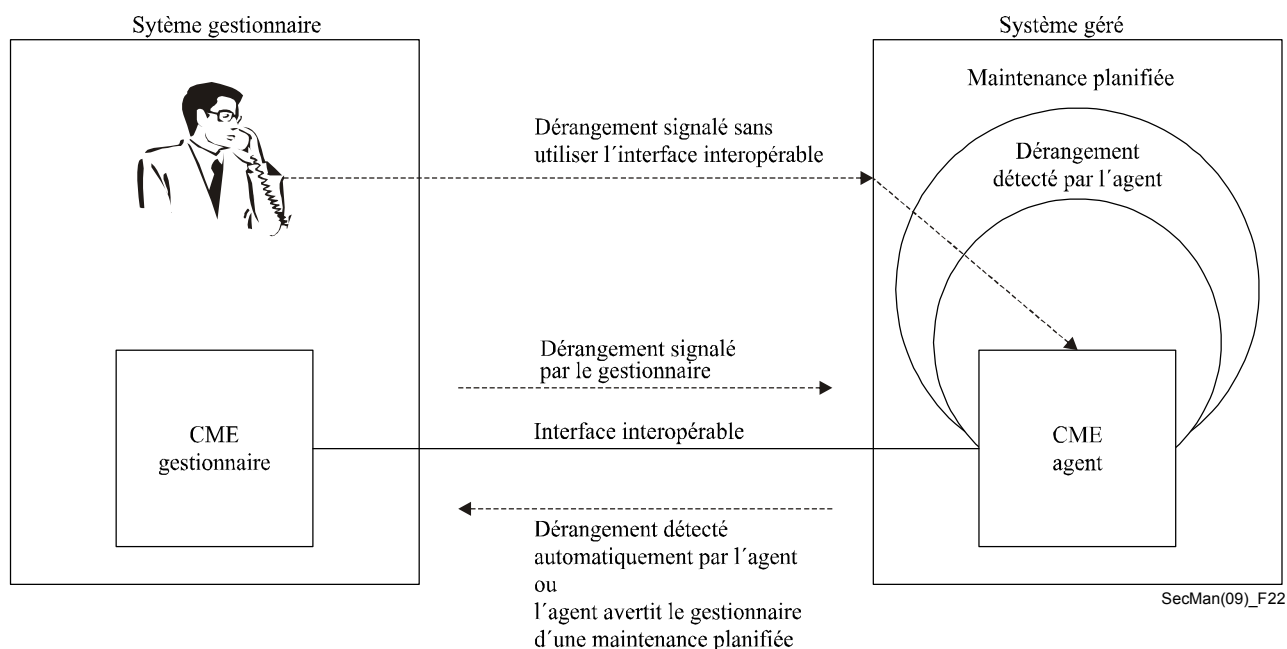


Figure 22 – Création d'un dossier de gestion de dérangement

La Recommandation UIT-T X.790, *Fonction de gestion des dérangements pour les applications de l'UIT-T*, définit cette application de gestion et utilise des mécanismes tels que les listes de contrôle d'accès et l'authentification bidirectionnelle pour sécuriser les activités.

7.6 Services communs de gestion de la sécurité

Un certain nombre de services communs sont considérés comme étant des activités du plan de gestion X.805. Ils s'appliquent en particulier lorsque le *protocole commun d'information de gestion (CMIP)* (Rec. UIT-T X.711) est utilisé. Ces services sont brièvement décrits ci-après.

7.6.1 Fonction de signalisation des alarmes de sécurité

La signalisation des alarmes est une fonction essentielle dans les interfaces de gestion. Lorsqu'une défaillance est détectée, par suite de problèmes opérationnels (par exemple défaillance de l'ensemble de circuits ou violation de la politique de sécurité), une alarme est communiquée au système de gestion. Les rapports d'alarme incluent un certain nombre de paramètres, de sorte que le système de gestion puisse déterminer le motif de la défaillance et prendre une mesure corrective. Les paramètres relatifs à un événement donné incluent un champ obligatoire appelé *type d'événement* et un ensemble d'autres champs appelés *informations d'événement*. Ces derniers champs contiennent des informations telles que la gravité de l'alarme, les motifs probables de déclenchement de l'alarme et le détecteur de la violation de sécurité. Les motifs de déclenchement des alarmes sont associés aux types d'événement comme indiqué dans le Tableau 6.

Tableau 6 – Motifs de déclenchement des alarmes de sécurité

Type d'événement	Motifs de déclenchement de l'alarme de sécurité
Violation de l'intégrité	Information dupliquée Information manquante Détection de modification d'information Information hors séquence Information inattendue
Violation opérationnelle	Refus de service Hors service Erreur de procédure Raison non spécifiée
Violation physique	Altération frauduleuse du câble Détection d'intrusion Raison non spécifiée
Violation de service ou de mécanisme de sécurité	Echec d'authentification Atteinte à la confidentialité Echec de non-répudiation Tentative d'accès non autorisée Raison non spécifiée
Violation du domaine temporel	Information tardive Mot de passe périmé Activité en dehors de l'horaire

On trouvera davantage d'explications sur ces motifs de déclenchement des alarmes dans la Rec. UIT-T X.736, *Fonction de signalisation des alarmes de sécurité*.

7.6.2 Fonction de piste de vérification de sécurité

Une piste de vérification de sécurité est utilisée pour enregistrer les événements relatifs à la sécurité et, en particulier, les violations de sécurité. Parmi les événements relatifs à la sécurité, on peut citer les connexions, les déconnexions, les utilisations de mécanismes de sécurité, les opérations de gestion et la comptabilisation de l'utilisation. La *fonction de piste de vérification de sécurité* est définie dans la Rec. UIT-T X.740.

7.6.3 Contrôle d'accès pour les entités gérées

La Rec. UIT-T X.741, *Objets et attributs de contrôle d'accès*, définit de façon très détaillée le modèle associé à l'attribution d'un certain contrôle d'accès aux diverses entités gérées. Cette Recommandation permet notamment de satisfaire aux spécifications suivantes: protéger les informations de gestion contre toute

création, suppression et modification non autorisées, faire en sorte que les opérations soient compatibles avec les droits d'accès de ceux qui sont à l'origine des opérations et empêcher la transmission d'informations de gestion à des destinataires non autorisés. Divers niveaux de contrôle d'accès sont définis pour respecter ces spécifications. Pour les opérations de gestion, des restrictions d'accès peuvent être appliquées à plusieurs niveaux. Une politique de contrôle d'accès peut être fondée sur un ou plusieurs des mécanismes définis (par exemple listes de contrôle d'accès, contrôle d'accès fondé sur des capacités, fondé sur des étiquettes et fondé sur des contextes). Dans le modèle défini dans la Rec. UIT-T X.741, la décision de permettre ou de refuser l'accès est fondée sur la politique de contrôle d'accès et sur les informations de contrôle d'accès (ACI, *access control information*). Les informations ACI sont par exemple constituées de règles, de l'identité du demandeur, des identités des cibles auxquelles l'accès est demandé et d'informations relatives à l'authentification du demandeur.

7.6.4 Services de sécurité fondés sur l'architecture CORBA

Tandis qu'un grand nombre des Recommandations UIT-T de la série X.700 reposent sur l'utilisation du protocole CMIP comme protocole aux interfaces de gestion, il existe d'autres tendances qui sont maintenant prises en compte dans ces Recommandations, en particulier l'utilisation d'un protocole, de services et de modèles d'objet fondés sur l'architecture de courtier commun de requêtes d'objets (CORBA) pour les interfaces de gestion. Il convient notamment de citer la Rec. UIT-T X.780, *Directives concernant le RGT pour la définition d'objets gérés CORBA*, la Rec. UIT-T X.780.1, *Directives concernant le RGT pour la définition d'interfaces d'objets gérés CORBA à granularité grossière*, la Rec. UIT-T X.780.2, *Lignes directrices relatives au RGT pour la définition d'objets gérés et d'objets de façade CORBA orientés services*, et la Rec. UIT-T X.781, *Spécifications et directives pour l'établissement de formulaires de déclaration de conformité d'implémentations associés aux systèmes de type CORBA*. De plus, la Recommandation UIT-T Q.816 définit un cadre pour l'utilisation de ces services dans le contexte des interfaces de gestion. En ce qui concerne la prise en charge des spécifications de sécurité pour ces interfaces, la Rec. UIT-T Q.816 renvoie à la spécification de l'OMG (*object management group*) relative aux services de sécurité communs.

8. Approches particulières relatives à la sécurité des réseaux

8 Approches particulières relatives à la sécurité des réseaux

Dans ce chapitre, les approches utilisées pour protéger divers types de réseau sont passées en revue. On commence par s'intéresser aux spécifications de sécurité pour les réseaux de prochaine génération, puis aux réseaux de communications mobiles qui passent d'une mobilité fondée sur une seule technologie (comme CDMA ou GSM) à une mobilité à travers des plateformes hétérogènes utilisant le protocole Internet. On examine ensuite les spécifications de sécurité pour les réseaux domestiques et la télévision par câble et enfin les problèmes de sécurité dans les réseaux de capteurs ubiquitaires.

8.1 Sécurité des réseaux de prochaine génération (NGN)

Un réseau de prochaine génération (NGN, *next generation network*) est un réseau en mode paquet qui est en mesure de fournir des services de télécommunication aux utilisateurs et d'utiliser de multiples technologies de transport à large bande à qualité de service imposée. De plus, les fonctions liées aux services sont indépendantes des technologies sous-jacentes liées au transport. Un NGN assure le libre accès des utilisateurs aux réseaux ainsi qu'aux services et fournisseurs de services concurrents. Il prend en charge la mobilité généralisée qui permet la fourniture cohérente et partout à la fois des services aux utilisateurs. On trouvera plus de détails sur les caractéristiques générales d'un NGN dans la Recommandation UIT-T Y.2001, *Aperçu général des réseaux de prochaine génération*.

8.1.1 Objectifs et spécifications de sécurité des NGN

La sécurité étant déterminante pour les NGN, il est essentiel de mettre en place un ensemble de normes qui garantiront le plus possible la sécurité des NGN. À mesure que les NGN évoluent et que de nouvelles vulnérabilités de sécurité apparaissent pour lesquelles aucun remède automatique immédiat n'est connu, ces vulnérabilités doivent être décrites correctement de manière à ce que les administrateurs de réseau et les utilisateurs finals puissent en limiter les effets.

Les études relatives à la sécurité des NGN doivent donner lieu à la définition d'architectures de réseau qui:

- assurent une protection maximale des ressources des réseaux et des utilisateurs finals;
- permettent une forte répartition de l'intelligence de bout en bout;
- permettent à de multiples technologies de mise en réseau de coexister;
- prennent en charge des mécanismes de sécurité de bout en bout;
- prennent en charge des solutions de sécurité qui s'appliquent sur plusieurs domaines administratifs;
- prennent en charge une gestion d'identité sécurisée, et notamment (la liste n'est pas exhaustive):
 - l'authentification fiable des entités des NGN (par exemple les utilisateurs, les dispositifs d'utilisateur, les fournisseurs de réseau, les fournisseurs de service, les fournisseurs d'identité, etc.);
 - la garantie que seules les entités autorisées peuvent accéder aux données d'identité dans les NGN;
 - l'échange sécurisé d'informations d'identité entre entités fédérées dans les NGN;
 - la possibilité de garder en mémoire l'utilisation des informations d'identité dans les NGN;
 - la prise en charge du respect de la vie privée des utilisateurs et de l'anonymat dans les NGN; et
 - l'assistance des utilisateurs NGN pour les aider à gérer leurs informations d'identité en toute sécurité (par exemple modification de profils d'utilisateur, modification de mots de passe, activation de services basés sur l'emplacement, visualisation des relevés de facturation, etc.);

- prennent en charge des solutions de sécurité pour la TVIP qui sont performantes et ont un impact acceptable sur la qualité de fonctionnement, la qualité de service, l'utilisabilité et l'évolutivité. Parmi les types de protection que la sécurité de la TVIP devrait garantir, on peut citer (la liste n'est pas exhaustive):
 - la protection des contenus;
 - la protection des services;
 - la protection des réseaux;
 - la protection des terminaux; et
 - la protection des abonnés.

La Recommandation UIT-T Y.2701, *Prescriptions de sécurité des réseaux de prochaine génération de version 1*, qui s'appuie sur les principes énoncés dans la Rec. UIT-T X.805, énonce des spécifications de sécurité pour protéger les NGN contre les menaces de sécurité et examine certains aspects techniques de la gestion d'identité.

Les éléments suivants doivent être protégés dans un environnement multi-réseaux:

- l'infrastructure des fournisseurs de réseau et de service et les actifs (par exemple les actifs et les ressources des NGN tels que les éléments de réseau, les systèmes, les composants, les interfaces, les données et les informations), les ressources, les communications (à savoir le trafic de signalisation, de gestion et de données/support) et les services associés;
- les services et capacités des NGN (par exemple les services voix, vidéo et données); et
- les communications des utilisateurs finals et les informations les concernant (par exemple les informations privées).

Les spécifications doivent assurer la sécurité des communications des utilisateurs finals à travers plusieurs domaines administratifs de réseau, comme illustré sur la Figure 23.

Les spécifications énoncées dans la Rec. UIT-T Y.2701 sont considérées comme un ensemble minimal de spécifications. Un fournisseur NGN peut être amené à prendre des mesures complémentaires à celles qui sont spécifiées.

La multiplicité des réseaux augmente les risques de menaces telles que l'interception illégale de profils d'utilisateur, de contenus (par exemple communications vocales ou de données) et d'informations d'authentification.

Les télécommunications mobiles internationales 2000 (IMT-2000) constituent la norme mondiale pour les communications sans fil de troisième génération (3G). Définies par un ensemble de Recommandations interdépendantes de l'UIT, les IMT-2000 constituent un cadre pour l'accès sans fil dans le monde entier grâce à l'interconnexion des divers systèmes de réseaux de Terre et/ou à satellite. Elles exploiteront la synergie potentielle entre les technologies de télécommunications mobiles numériques et les systèmes d'accès sans fil fixes et mobiles.

Les activités de l'UIT sur les IMT-2000 comprennent une normalisation internationale ainsi que l'attribution de bandes de fréquences et des spécifications techniques pour les composants radio et réseau, la tarification et la facturation, une assistance technique et des études sur les aspects réglementaires et politiques.

Les spécifications générales de sécurité des réseaux IMT-2000 font l'objet des Recommandations UIT-T Q.1701, *Cadre général des réseaux IMT-2000*, UIT-T Q.1702, *Aspects réseau au-delà des systèmes IMT-2000 – Vision à long terme* et UIT-T Q.1703, *Cadre général des capacités de service et de réseau des aspects réseau des systèmes au-delà de l'IMT-2000*.

En outre, les spécifications 3G énoncées dans les séries de Recommandations UIT-T Q.1741 (3GPP) et UIT-T Q.1742 (3GPP2) contiennent une évaluation des menaces perçues et une liste de spécifications de sécurité pour prendre en compte ces menaces. Ces Recommandations contiennent aussi des objectifs et des principes de sécurité pour les communications mobiles, la définition d'une architecture de sécurité, la spécification d'algorithmes cryptographiques, les conditions de l'interception licite ainsi que l'architecture et les fonctions de l'interception licite.

8.2.1 Communications mobiles sécurisées de données de bout en bout

Les terminaux mobiles dotés de capacités de communication de données (téléphones mobiles IMT-2000, ordinateurs personnels portables, PDA avec carte radio, etc.) sont très répandus, et divers services d'application (par exemple commerce électronique) utilisent des terminaux raccordés au réseau mobile. Pour les applications commerciales comme pour la protection de l'utilisateur final, la sécurité est essentielle.

Les réseaux mobiles sont particulièrement vulnérables du fait de la nature du réseau sans fil et des vulnérabilités intrinsèques des technologies de communication sans fil. La sécurité doit être prise en considération du point de vue de l'opérateur de réseau mobile, du fournisseur de service d'application et de l'utilisateur final. La sécurité entre le terminal mobile et le serveur d'application est particulièrement importante. En ce qui concerne les communications mobiles de bout en bout, l'UIT-T a élaboré un ensemble complet de solutions de sécurité, dont certaines sont examinées ci-dessous.

8.2.1.1 Cadre pour les communications mobiles sécurisées de données de bout en bout

La Recommandation UIT-T X.1121, *Cadre général des technologies de la sécurité pour les communications mobiles de données de bout en bout*, décrit deux modèles de communications mobiles de données de bout en bout entre un utilisateur mobile et un fournisseur de service d'application (ASP, *application service provider*): un modèle général et un modèle avec passerelle, comme illustré sur les Figures 24 et 25. Le fournisseur ASP fournit le service aux utilisateurs mobiles par le biais du serveur d'application. Dans le modèle avec passerelle, la passerelle de sécurité sert de relais pour les paquets entre le terminal mobile et le serveur d'application et convertit un protocole de communication fondé sur le réseau mobile en un protocole fondé sur un réseau ouvert, et inversement. La Figure 26 décrit les menaces concernant les communications mobiles de données de bout en bout. La Figure 27 indique les endroits où des fonctions de sécurité sont nécessaires pour chaque entité et la relation entre les entités.

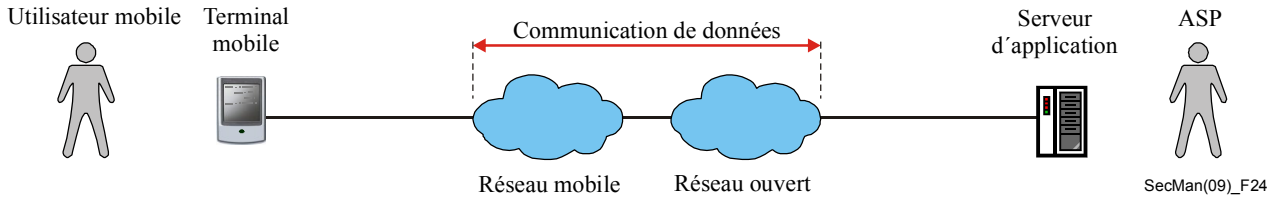


Figure 24 – Modèle général pour les communications mobiles de données de bout en bout entre un utilisateur mobile et un ASP

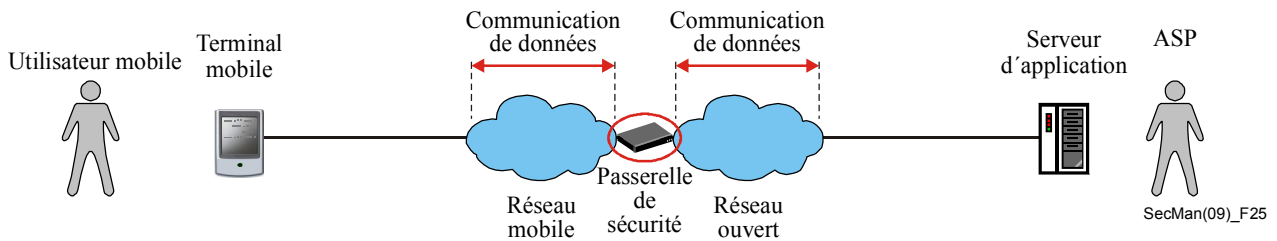


Figure 25 – Modèle avec passerelle pour les communications mobiles de données de bout en bout entre un utilisateur mobile et un ASP

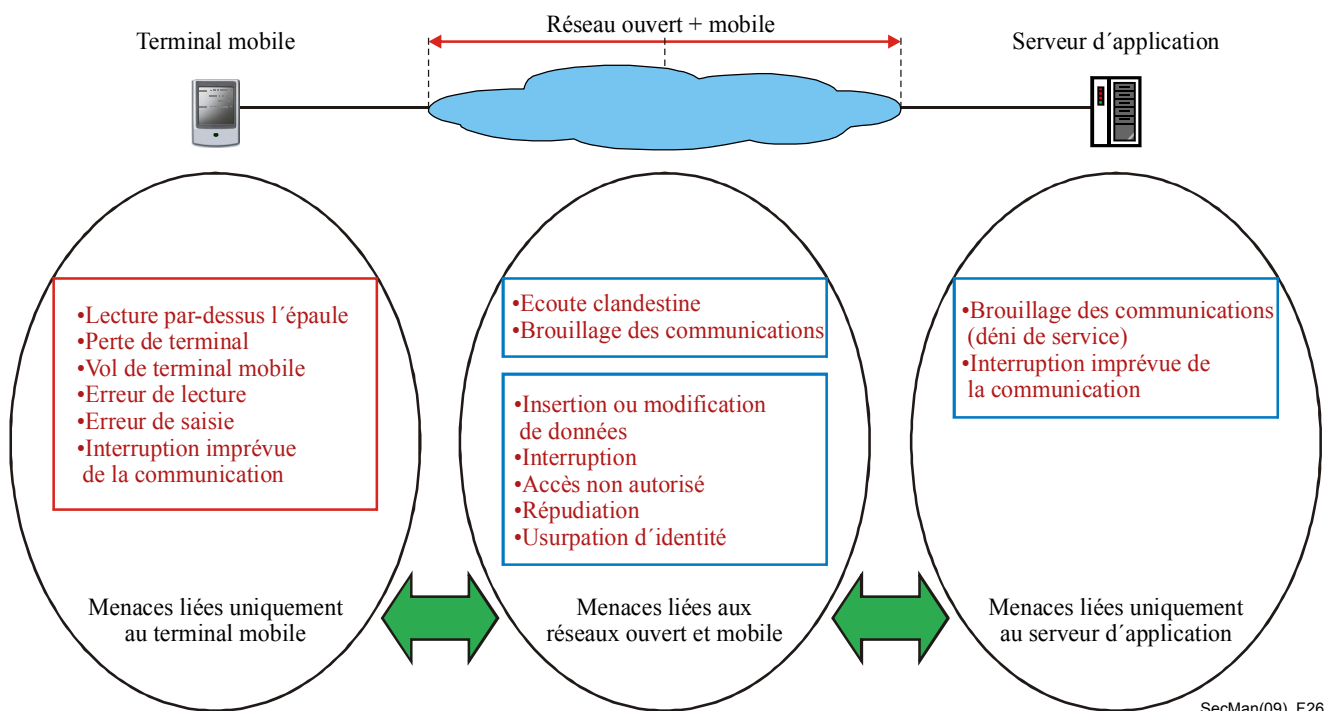


Figure 26 – Menaces concernant les communications mobiles de bout en bout

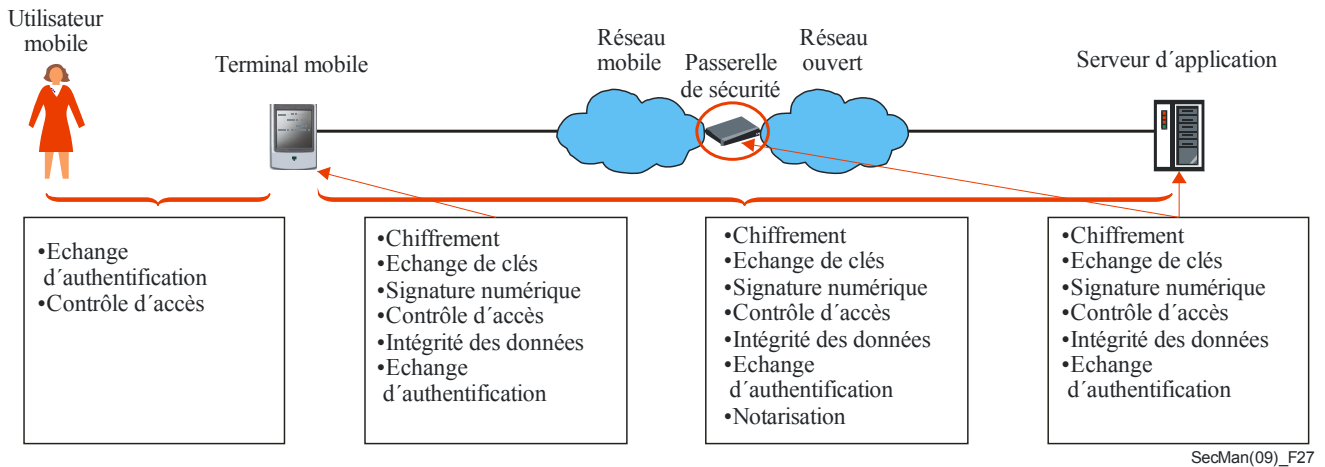
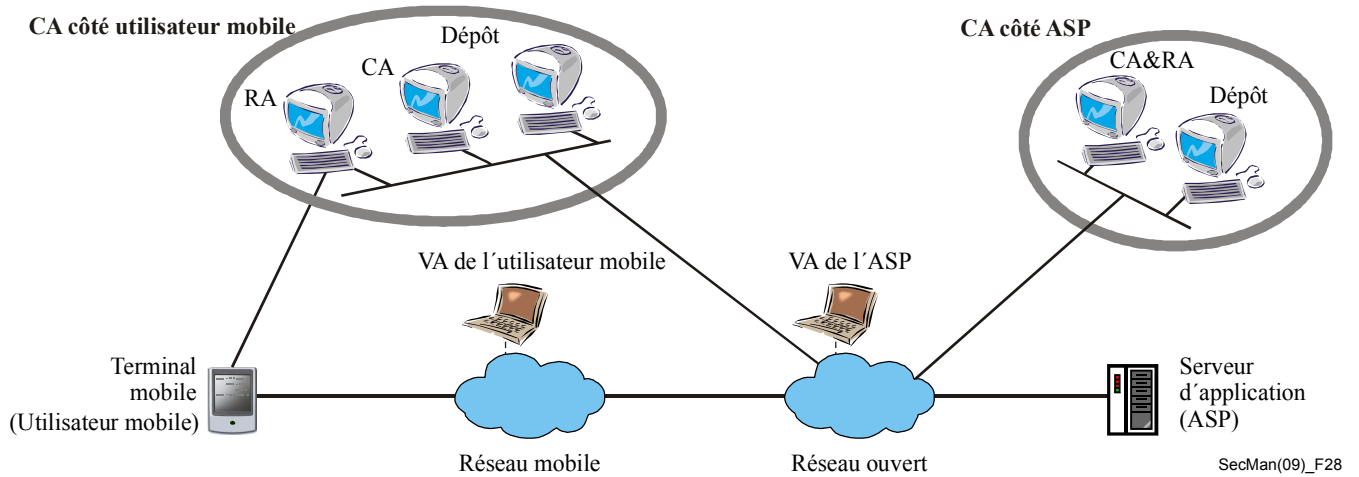


Figure 27 – Fonction de sécurité requise pour chaque entité et relation entre les entités

8.2.1.2 Architecture PKI pour les communications mobiles sécurisées de données de bout en bout

L'architecture PKI est très utile pour la fourniture de certaines fonctions de sécurité (par exemple confidentialité, signature numérique, intégrité des données) nécessaires pour les communications mobiles de données de bout en bout mais une certaine adaptation est nécessaire en raison des caractéristiques des communications mobiles de données. Des indications sur la mise en œuvre de l'architecture PKI dans un environnement mobile sont données dans la Rec. UIT-T X.1122, *Lignes directrices pour la réalisation de systèmes mobiles sécurisés basés sur l'infrastructure de clé publique (PKI)*, qui décrit à la fois un modèle PKI général et un modèle PKI avec passerelle.

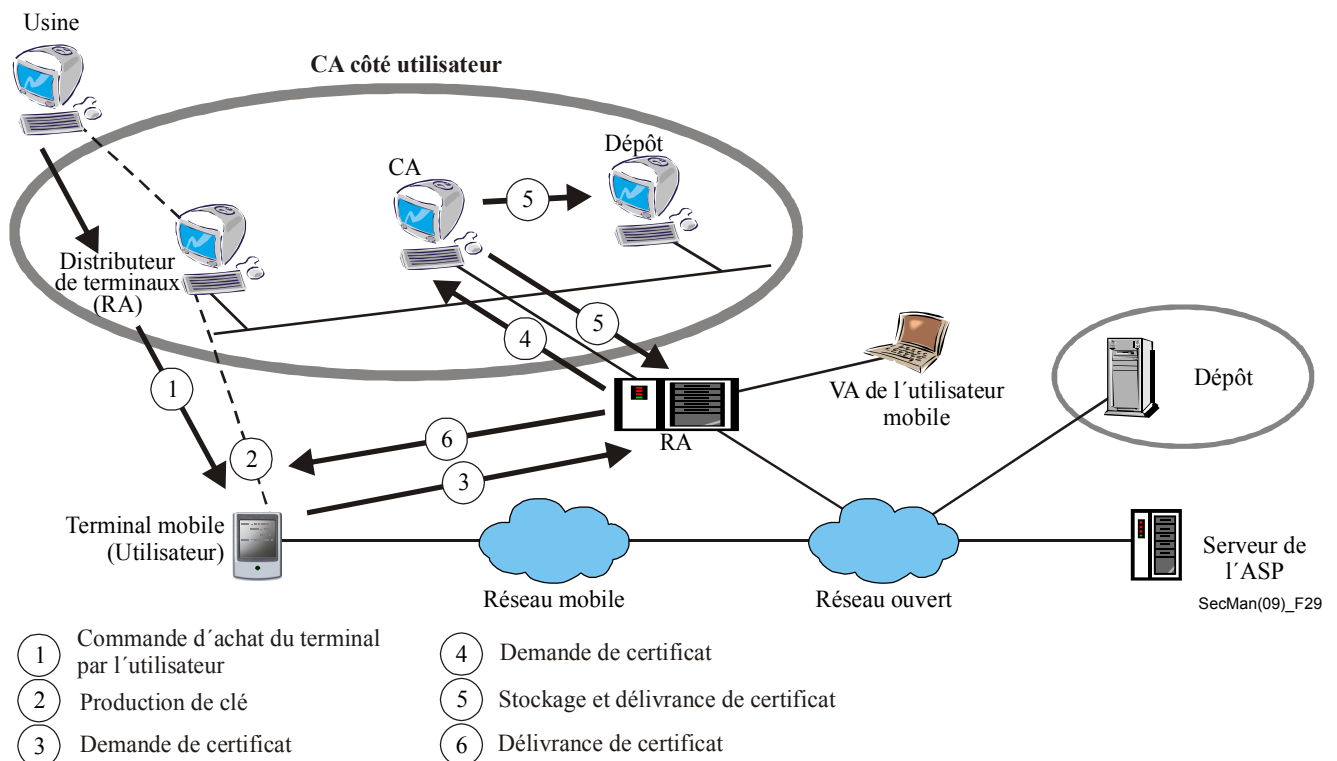
Dans le modèle général (illustré sur la Figure 28), l'autorité de certification (CA, *certification authority*) de l'utilisateur mobile délivre le certificat de l'utilisateur et gère le dépôt et la liste de révocation de certificats (CRL, *certificate revocation list*). L'autorité de validation (VA, *Validation Authority*) de l'utilisateur mobile fournit un service de validation de certificat en ligne à l'utilisateur mobile. L'autorité de certification du fournisseur ASP délivre le certificat du fournisseur ASP et gère le dépôt du fournisseur ASP et la liste CRL. L'autorité de validation du fournisseur ASP assure un service de validation de certificat en ligne pour les certificats de fournisseur ASP.



SecMan(09)_F28

Figure 28 – Modèle PKI général pour les communications mobiles de bout en bout

Il existe deux méthodes de délivrance de certificat suivant l'endroit où les clés publique/privée sont produites. Dans la première méthode, la paire de clés de chiffrement est produite dans l'usine de fabrication du terminal mobile; dans la deuxième méthode, la paire de clés de chiffrement est produite dans le terminal mobile ou dans un jeton infraudable rattaché au terminal mobile. La Figure 29 illustre la procédure d'acquisition d'un certificat par un terminal mobile, dans laquelle la paire de clés de chiffrement est produite dans le terminal mobile.



SecMan(09)_F29

Figure 29 – Procédure de délivrance de certificat pour le terminal mobile

Le terminal mobile dispose d'une puissance de calcul et d'une taille de mémoire limitées. Par conséquent, il est préférable de procéder à une validation de certificat en ligne plutôt qu'à une validation de certificat hors ligne sur la base d'une liste CRL. La Figure 30 illustre la procédure de validation de certificat en ligne pour un terminal mobile.

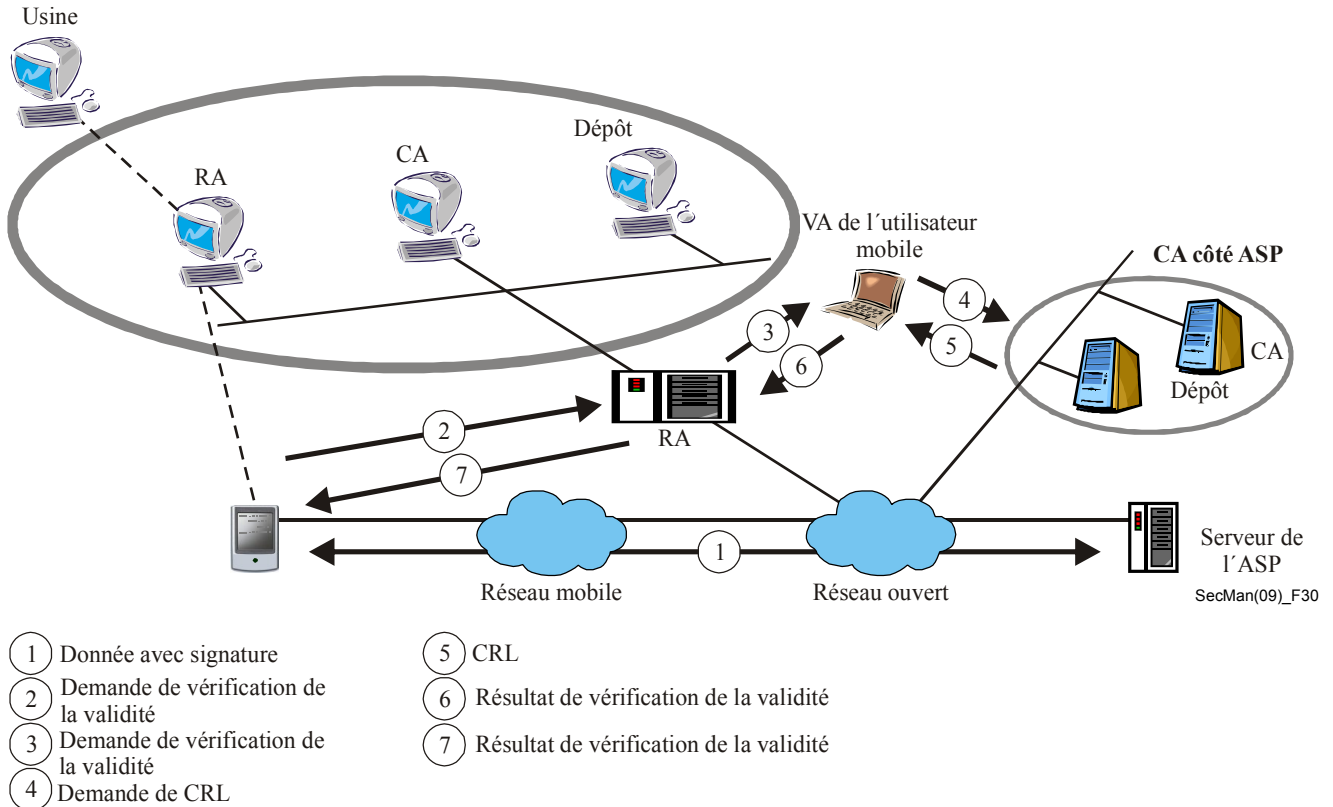


Figure 30 – Validation de certificat pour les communications mobiles de données de bout en bout

L'architecture PKI pour les communications mobiles de bout en bout peut être utilisée soit au niveau de la couche session, où elle peut prendre en charge des services de sécurité (par exemple authentification de client, authentification de serveur, confidentialité et intégrité), soit au niveau de la couche application, où elle peut prendre en charge des services de non-répudiation et de confidentialité.

8.2.1.3 Système de réaction corrélative pour les communications mobiles de données

Le système de réaction corrélative a été conçu pour permettre aux terminaux ou dispositifs mobiles et au réseau de coopérer dans la lutte contre les menaces de sécurité. La Recommandation UIT-T X.1125 décrit l'architecture générique d'un système de réaction corrélative dans lequel un réseau mobile et ses terminaux d'utilisateur peuvent interagir afin de combattre diverses menaces de sécurité pour les communications sécurisées de données de bout en bout. Parmi ces menaces, on peut notamment citer les virus, vers, chevaux de Troie ou d'autres menaces de réseau pesant à la fois sur le réseau mobile et sur ses utilisateurs.

Cette architecture offre aux réseaux d'opérateur une capacité de sécurité améliorée grâce à des mises à jour de sécurité dans les stations mobiles, un contrôle d'accès au réseau et des restrictions relatives aux services d'application. Il en résulte un mécanisme qui empêche aux virus ou aux vers de se propager rapidement à travers le réseau d'opérateur.

8.3 Sécurité des réseaux domestiques

Etant donné qu'un réseau domestique utilise diverses techniques de transmission filaires ou sans fil, il est exposé à des menaces analogues à celles auxquelles est exposé n'importe quel autre réseau filaire ou sans fil. Pour protéger le réseau domestique contre ces menaces, l'UIT-T a élaboré un ensemble complet de solutions, dont certaines sont examinées ci-après.

8.3.1 Cadre de sécurité pour les réseaux domestiques

La Recommandation UIT-T X.1111, *Cadre général des technologies de sécurité pour les réseaux domestiques*, s'appuie sur le modèle de menaces décrit dans la Rec. UIT-T X.1121 pour établir un cadre de sécurité pour les réseaux domestiques. Les caractéristiques du réseau domestique peuvent être résumées comme suit:

- divers supports de transmission peuvent être utilisés dans le réseau;
- le réseau peut utiliser des technologies filaires et/ou sans fil;
- il existe de nombreux environnements possibles à prendre en considération du point de vue de la sécurité;
- des utilisateurs distants peuvent transporter avec eux des terminaux distants; et
- les divers types de dispositif de réseau domestique nécessitent des niveaux de sécurité différents.

Le modèle général de réseau domestique pour la sécurité, qui est illustré sur la Figure 31, peut comprendre de nombreux dispositifs (PDA, PC et téléviseur/magnétoscope par exemple). Dans ce modèle, les dispositifs domestiques sont classés en trois types:

- les dispositifs de type A (télécommandes, PC ou PDA par exemple), qui ont la capacité de commander un dispositif de type B ou de type C;
- les dispositifs de type B sont des ponts qui connectent des dispositifs de type C (qui n'ont pas d'interface de communication) au réseau, autrement dit, un dispositif de type B communique avec d'autres dispositifs dans le réseau au moyen d'un langage propriétaire ou d'un mécanisme de commande; et
- les dispositifs de type C (caméras de sécurité, dispositifs audio/vidéo par exemple), qui fournissent un service aux autres dispositifs.

Certains dispositifs combinent les fonctions de type A et de type C.

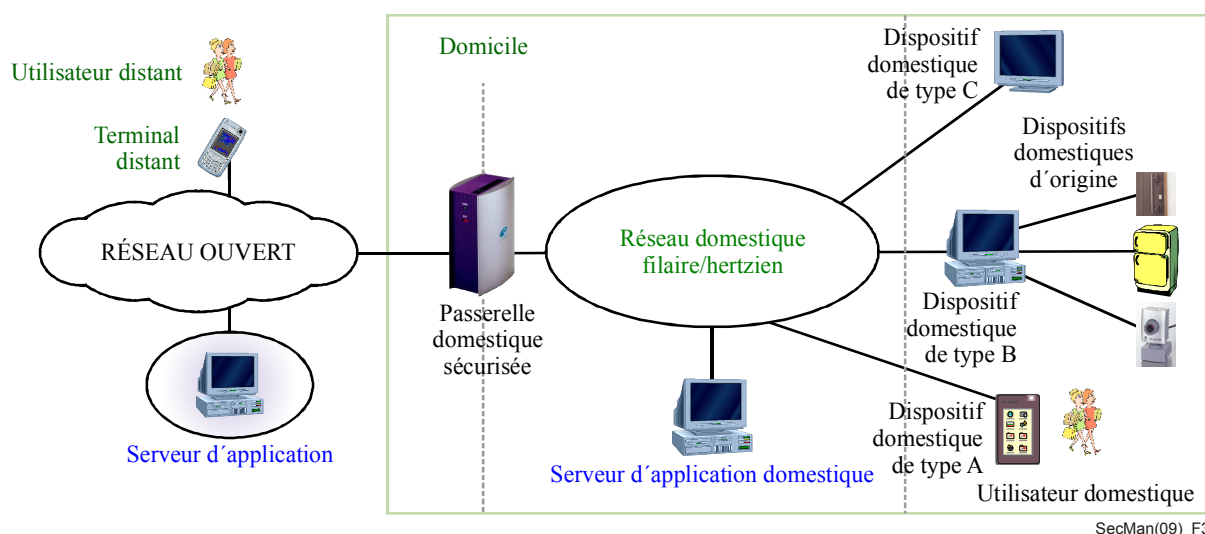


Figure 31 – Modèle général de réseau domestique pour la sécurité

La Recommandation UIT-T X.1111 décrit les menaces de sécurité et les spécifications de sécurité du point de vue de l'utilisateur domestique et de l'utilisateur distant. De plus, elle classe les technologies de sécurité selon les fonctions satisfaisant aux spécifications de sécurité et selon l'endroit où ces technologies doivent être appliquées.

8.3.2 Certification et authentification de dispositif dans les réseaux domestiques

Il existe deux options pour la certification de dispositif dans le réseau domestique: le modèle de délivrance externe, dans lequel tous les certificats de dispositif domestique sont délivrés par une autorité de certification (CA) externe, et le modèle de délivrance interne, dans lequel les certificats de dispositif (y compris les certificats autosignés et les certificats d'entité finale) sont délivrés par une autorité de certification interne au réseau domestique. En règle générale, une autorité de certification interne est une passerelle domestique sécurisée capable de générer une paire de clés et de délivrer un certificat, autrement dit, la passerelle domestique peut délivrer à la fois un certificat d'autorité de certification et des certificats de dispositif domestique. La passerelle domestique sécurisée proprement dite peut avoir un certificat de dispositif qui est délivré par une autorité de certification externe pour utilisation dans des services externes. Ce certificat de dispositif délivré en externe pour la passerelle domestique peut être utilisé pour l'authentification entre la passerelle domestique et le fournisseur de service de réseau.

La Recommandation UIT-T X.1112 décrit un cadre pour le modèle interne de délivrance, de gestion et d'utilisation de certificat de dispositif pour les réseaux domestiques. Ce modèle est illustré sur la Figure 32.

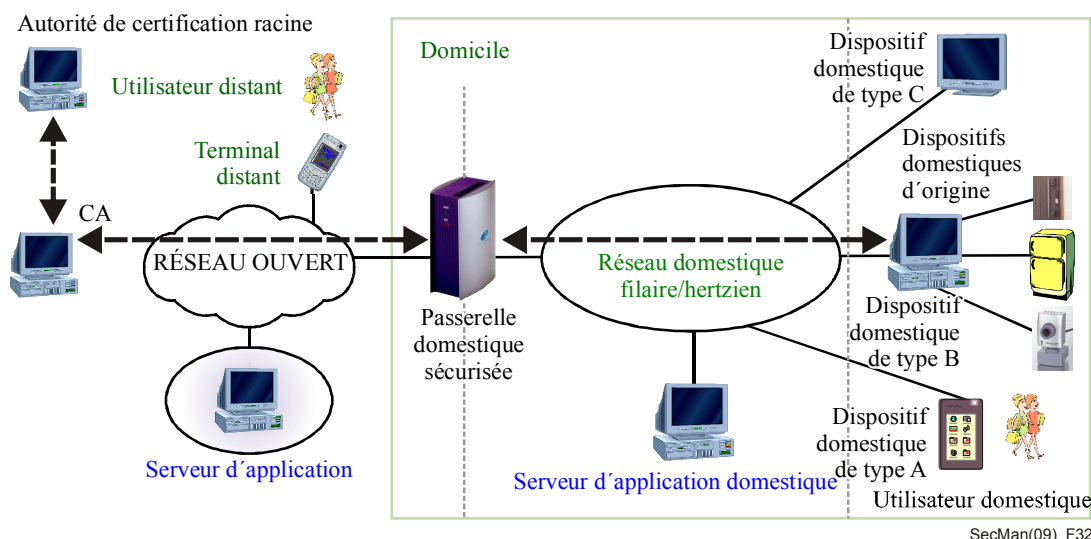


Figure 32 – Modèle d'authentification de dispositif pour le réseau domestique sécurisé

Pour l'authentification de dispositif, un identificateur unique est nécessaire pour chaque dispositif du réseau domestique. Plus précisément, un certificat de dispositif domestique sera nécessaire en tant qu'élément de confiance unique lorsque le dispositif est utilisé dans le réseau domestique.

La Figure 33 illustre quatre scénarios types d'utilisation d'un certificat de dispositif: 1) entre le terminal distant et la passerelle domestique sécurisée, 2) entre le serveur d'application et la passerelle domestique sécurisée; 3) entre les dispositifs domestiques et la passerelle domestique sécurisée; et 4) entre deux dispositifs domestiques.

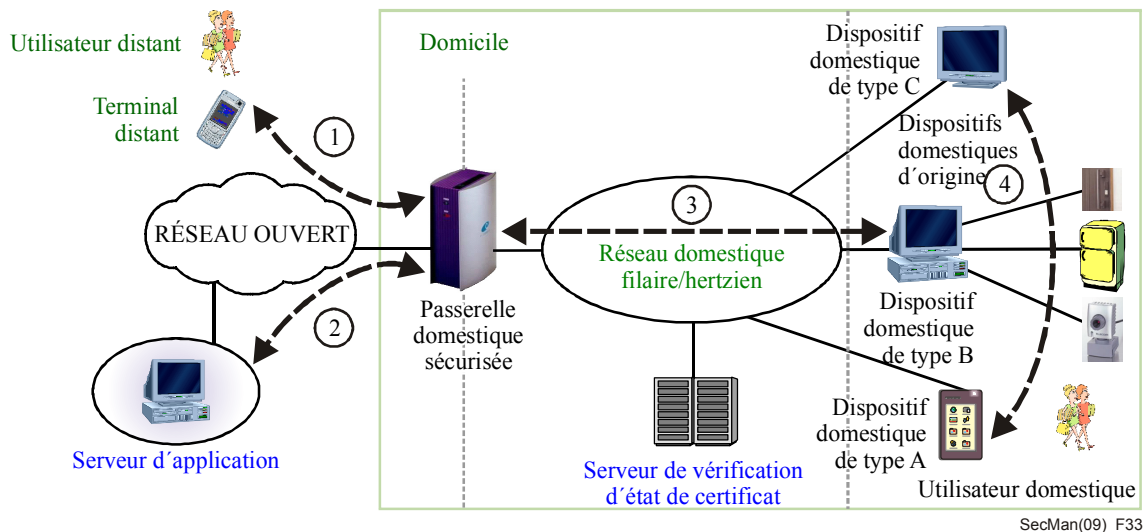


Figure 33 – Scénarios d'utilisation de l'authentification de dispositif basés sur le modèle général de réseau domestique pour la sécurité

Pour un service Internet externe entre le dispositif domestique et le serveur d'application externe, le dispositif domestique doit d'abord s'authentifier auprès de la passerelle domestique sécurisée en utilisant son propre certificat de dispositif. La passerelle domestique sécurisée doit ensuite s'authentifier auprès du serveur d'application externe en utilisant le certificat de passerelle domestique délivré par une autorité de certification externe. Ces scénarios d'utilisation peuvent être appliqués à divers protocoles d'application pour la prise en charge de services de réseau domestique sécurisés.

8.3.3 Authentification des utilisateurs humains pour les services de réseau domestique

Certains environnements exigent l'authentification de l'utilisateur humain et non d'un processus ou d'un dispositif et, pour cela, les utilisateurs humains doivent prouver leur caractère unique, qui est généralement fondé sur des caractéristiques telles que quelque chose que l'utilisateur connaît, quelque chose qu'il possède ou une certaine caractéristique immuable de l'utilisateur.

La Recommandation UIT-T X.1113 donne des indications sur l'authentification d'utilisateur pour le réseau domestique fondée sur diverses techniques (par exemple mots de passe, certificats et données biométriques). Elle définit également le niveau de garantie de sécurité et le modèle d'authentification suivant les scénarios de service d'authentification. La Figure 34 représente les flux de service d'authentification sur la base du modèle général de sécurité du réseau domestique défini dans la Rec. UIT-T X.1111. Dans cet exemple, un utilisateur distant essaie d'accéder à des entités situées à l'intérieur du domicile, tandis que l'utilisateur domestique essaie d'accéder à des entités situées à l'intérieur ou à l'extérieur du domicile.

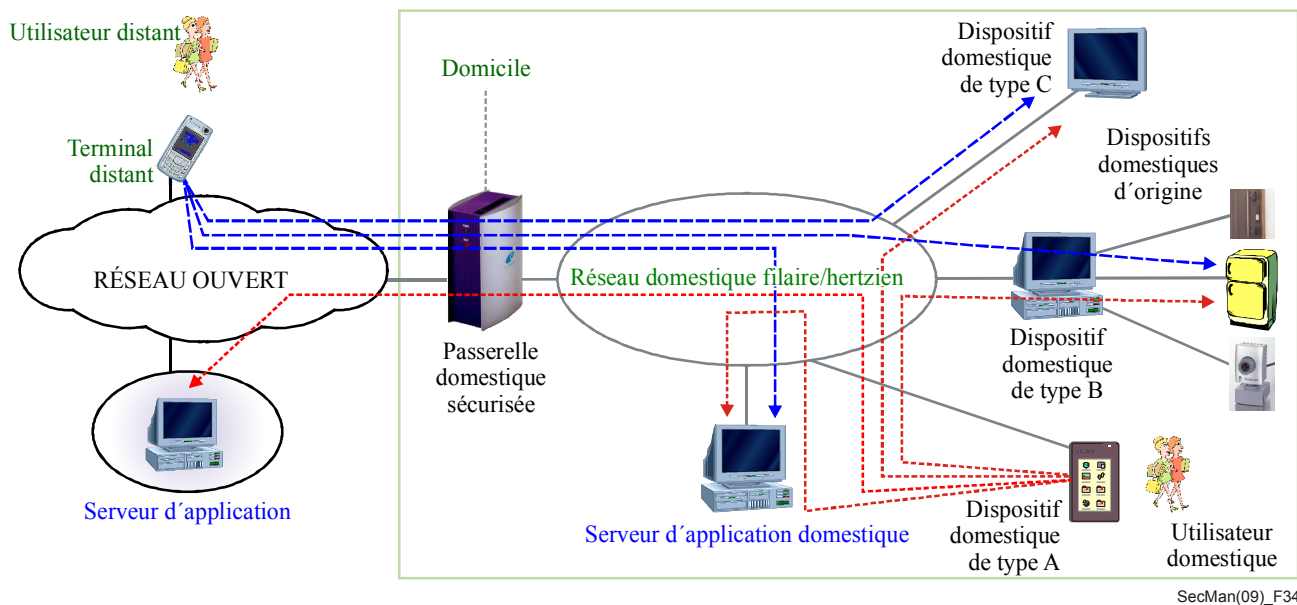


Figure 34 – Flux de service d'authentification pour le réseau domestique

8.4 IPCablecom

Le système IPCablecom permet aux opérateurs de télévision par câble d'offrir des services basés sur IP en temps réel (par exemple des communications téléphoniques) sur des réseaux qui ont été améliorés pour prendre en charge des câblo-modems.

8.4.1 Architecture IPCablecom

L'architecture IPCablecom est définie dans la Recommandation UIT-T J.160. Les composants IPCablecom sont illustrés sur la Figure 35. L'architecture IPCablecom contient à la fois des éléments de réseau sécurisés et des éléments de réseau non sécurisés. Normalement, les éléments de réseau sécurisés sont situés dans le cœur de réseau géré d'un câblo-opérateur. Les éléments de réseau non sécurisés, comme les câblo-modems et les adaptateurs de terminal média (MTA, *media terminal adapter*), sont normalement situés en dehors des installations du câblo-opérateur, chez l'abonné.

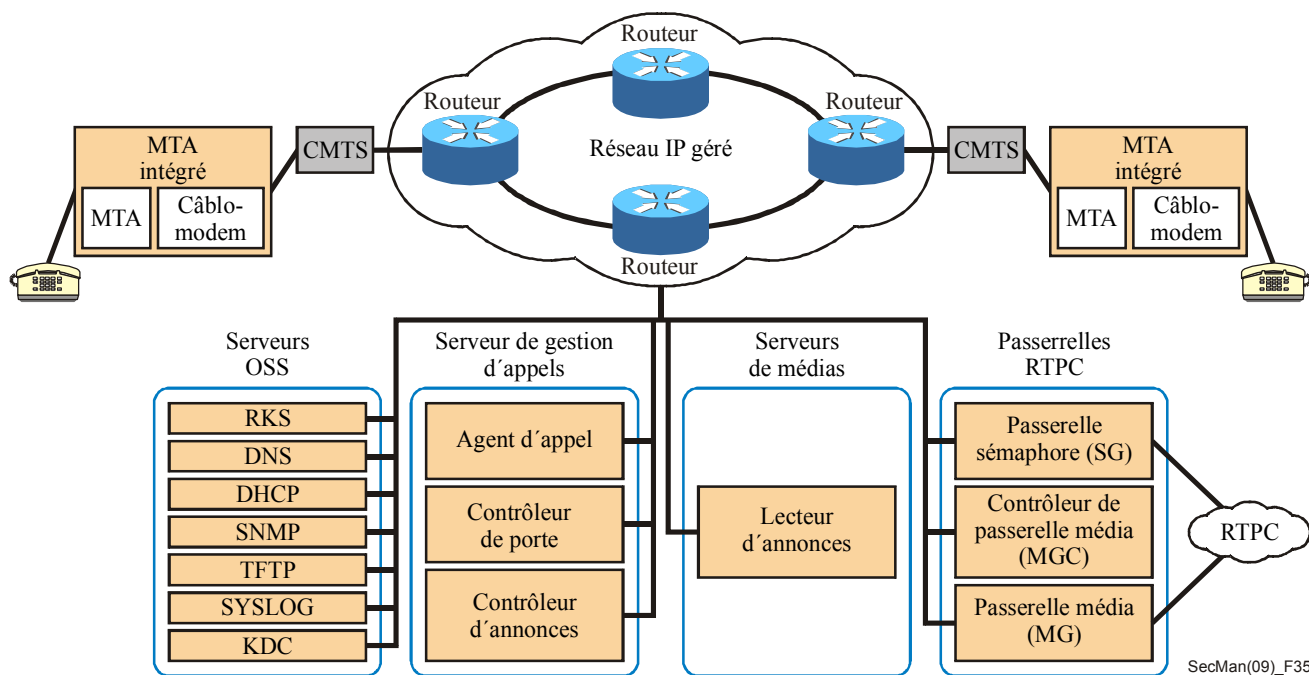


Figure 35 – Modèle de référence des composants IPCablecom

8.4.2 Spécifications de sécurité pour IPCablecom

Chacune des interfaces de protocole IPCablecom est exposée à des menaces qui peuvent affecter à la fois l'abonné et le fournisseur de service. Par exemple, le trajet du flux de média peut passer par un grand nombre de fournisseurs de service Internet et de réseau dorsal potentiellement inconnus. Le flux de média peut alors être vulnérable aux écoutes clandestines, lesquelles entraînent une perte de la confidentialité des communications. Les objectifs de conception de la sécurité identifiés dans l'architecture IPCablecom sont les suivants:

- permettre des capacités vocales résidentielles avec au moins le même niveau perçu de respect de la vie privée que dans le cas du RTPC;
- assurer une protection contre les attaques visant les adaptateurs MTA; et
- assurer une protection du câblo-opérateur contre les interruptions de réseau et les attaques par déni de service ou par vol de service.

Pour la conception, il faut prendre en compte la confidentialité, l'authentification, l'intégrité et le contrôle d'accès.

Les spécifications de sécurité sont énoncées dans la Recommandation UIT-T J.170, *Spécification de la sécurité sur IPCablecom*. Les menaces à prendre en compte sont récapitulées ci-dessous:

- vol de service, qui comprend: la fraude à l'abonnement, le non-paiement de services, les clones d'adaptateur MTA (par exemple lorsqu'un adaptateur MTA enregistré sous un compte frauduleux est cloné), l'usurpation de l'identité d'un serveur de réseau et la manipulation de protocole;
- divulgation d'informations de canal support, qui comprend: le simple espionnage, les clones d'adaptateur MTA (par exemple d'un adaptateur MTA accessible par le grand public), la manipulation de protocole, l'analyse cryptographique hors ligne et l'interruption de service;
- divulgation d'informations de signalisation;

- vol de services fondés sur les adaptateurs MTA; et
- enregistrement illégal d'un adaptateur MTA loué auprès d'un fournisseur de service différent.

8.4.3 Services et mécanismes de sécurité dans IPCablecom

Dans le système IPCablecom, la sécurité est implémentée dans les éléments les plus bas de la pile et utilise donc essentiellement des mécanismes définis par l'IETF. L'architecture IPCablecom fait face aux menaces en spécifiant, pour chaque interface de protocole définie, les mécanismes de sécurité sous-jacents (tels que IPsec) qui offrent à l'interface les services de sécurité dont elle a besoin. Dans le contexte de l'architecture X.805, les services de sécurité définis pour IPCablecom concernent les neuf cellules résultant des trois plans et des trois couches de la Figure 1.

Les services de sécurité disponibles par l'intermédiaire de la couche des services essentiels de l'architecture IPCablecom sont les suivants: authentification, contrôle d'accès, intégrité, confidentialité et non-répudiation. Les mécanismes de sécurité comprennent à la fois le protocole de sécurité (par exemple IPsec, sécurité de couche RTP et sécurité SNMPv3) et le protocole de gestion de clés support (par exemple IKE, PKINIT/Kerberos). Par ailleurs, les services essentiels de sécurité IPCablecom incluent un mécanisme assurant le chiffrement de bout en bout des flux de média RTP, ce qui réduit fortement la menace de perte de confidentialité.

8.5 IPCablecom2

IPCablecom2 est une initiative du secteur du câble destinée à favoriser la convergence de la voix, de la vidéo, des données et des technologies de mobilité.

8.5.1 Architecture IPCablecom2

IPCablecom2 est fondé sur la version 6 du sous-système multimédia IP (IMS, *IP multimedia subsystem*) définie dans le cadre du projet de partenariat pour la troisième génération (3GPP). Le 3GPP a notamment pour objet de produire des spécifications techniques pour le GSM et les réseaux de systèmes mobiles de la troisième génération (3G) et d'élaborer une architecture de communications IP fondées sur le protocole SIP pour les réseaux mobiles. L'architecture résultante, le *sous-système multimédia IP*, constitue la base de l'architecture IPCablecom2 définie dans la Rec. UIT-T J.360.

8.5.2 Spécifications de sécurité pour IPCablecom2

Les objectifs nominaux de l'architecture de sécurité IPCablecom2 sont les suivants:

- prise en charge de la confidentialité, de l'authentification, de l'intégrité et des mécanismes de contrôle d'accès;
- protection du réseau contre les attaques par déni de service, interruption du réseau et vol de service;
- protection des équipements d'utilisateur (UE) (c'est-à-dire des clients) contre les attaques par déni de service, les failles de sécurité et l'accès non autorisé depuis le réseau;
- prise en charge du respect de la vie privée de l'utilisateur final par l'intermédiaire du chiffrement et de mécanismes de contrôle d'accès aux données de l'abonné telles que les informations de présence;
- mécanismes d'authentification des dispositifs, des équipements UE et des utilisateurs et mise en service, signalisation et téléchargement logiciel sécurisés;
- exploitation et extension de l'architecture de sécurité du sous-système IMS pour promouvoir les objectifs énoncés précédemment.

Les menaces générales contre la sécurité d'IPCablecom2 sont les suivantes:

Menaces concernant le domaine de confiance

Un domaine de confiance est un groupement logique d'éléments de réseau qui sont sécurisés pour les communications. On peut délimiter les domaines de confiance au moyen de frontières physiques ou logiques. La communication entre les domaines de confiance doit toujours être protégée par authentification et autorisation. De plus, les interfaces qui connectent des éléments de réseau à l'intérieur d'un domaine, les interfaces entre domaines et les interfaces entre les équipements d'utilisateur et le fournisseur de service doivent être sécurisées contre diverses menaces.

Vol de service

Le vol de service peut être réalisé de diverses manières, en particulier (la liste n'est pas exhaustive): manipulation d'équipement d'utilisateur; exploitation de faille de protocole, usurpation d'identité, clonage d'équipement d'utilisateur (à savoir le fait d'imiter un équipement d'utilisateur légitime), fraude à l'abonnement et non-paiement de services.

Interruption et déni de service

On peut citer les attaques générales par déni de service, les attaques par inondation (visant à rendre indisponible un élément de réseau particulier, généralement en dirigeant une quantité excessive de trafic média dans le réseau au niveau de ses interfaces) et les attaques utilisant des zombies (à savoir de nombreux systèmes de point d'extrémité compromis).

Menaces contre le canal de signalisation

Dans un environnement multimédia, les messages de signalisation comprennent des données relatives à l'identité, aux services et au routage et d'autres données sensibles et critiques. Il existe des composants multimédias comme les proxys dans le domaine d'accès, ce qui les expose à un nombre accru de menaces. Les attaques contre la sécurité de la signalisation sont les suivantes: confidentialité compromise des informations de signalisation, attaques par intercepteur résultant de l'interception et de la modification possible du trafic transitant dans une communication entre deux parties et attaques par déni de service dans le canal de signalisation.

Menaces contre le canal support

Les menaces contre le canal support concernent le trafic média transféré entre les parties qui communiquent entre elles.

Menaces de sécurité propres au protocole

Il existe toute une variété de menaces contre chaque protocole multimédia.

8.5.3 Services et mécanismes de sécurité dans IPCablecom2

IPCablecom2 utilise largement la sécurité de couche transport et d'autres mécanismes dont il est question dans le sous-système multimédia IP 3GPP (3GPP 23.002 v6.10.0, *Network Architecture*, décembre 2005). Les paragraphes qui suivent résument les améliorations apportées à l'architecture de sécurité IMS par IPCablecom2.

8.5.3.1 Authentification d'utilisateur et d'équipement d'utilisateur

L'architecture IPCablecom2 prend en charge les mécanismes d'authentification suivants:

- authentification et concordance de clés fondées sur le sous-système multimédia IP;
- authentification fondée sur le condensé SIP (protocole d'ouverture de session); et
- amorçage par certificat.

L'architecture prend en charge les équipements d'utilisateur ayant plusieurs justificatifs d'authentification. Par exemple, un équipement d'utilisateur peut avoir un certificat pour accéder à des services lorsqu'il se trouve sur un réseau câblé, et une carte de circuit intégré universelle (UICC) pour accéder à des services lorsqu'il se trouve sur un réseau cellulaire.

Un abonné peut avoir plusieurs justificatifs. Un abonné peut avoir plusieurs équipements d'utilisateur, avec des capacités différentes liées à ces justificatifs. Par exemple, un abonné peut avoir un adaptateur MTA avec un certificat lorsqu'il est à son domicile, et un équipement d'utilisateur avec une carte UICC lorsqu'il est en déplacement.

8.5.3.2 Sécurité de la signalisation

IPCablecom2 ajoute la sécurité de couche transport (TLS, *transport layer security*) en tant qu'option pour la sécurité de la signalisation entre l'équipement d'utilisateur et la fonction proxy de commande de session d'appel. L'utilisation de TLS (telle qu'elle est définie dans le cadre du sous-système multimédia IP (IMS)) est facultative pour la sécurité de la signalisation.

8.6 Sécurité des réseaux de capteurs ubiquitaires

Un capteur est simplement un dispositif qui produit un signal électrique qui représente une propriété physique mesurable. Un réseau de capteurs ubiquitaires (USN, *Ubiquitous Sensor Network*) est un réseau qui utilise des capteurs à faible coût et à faible puissance pour développer la perception du contexte afin de communiquer des données captées à toute personne, où qu'elle se trouve et à tout moment. Un réseau USN peut couvrir une grande zone géographique et peut prendre en charge diverses applications. La Figure 36 illustre les applications potentielles des réseaux USN.

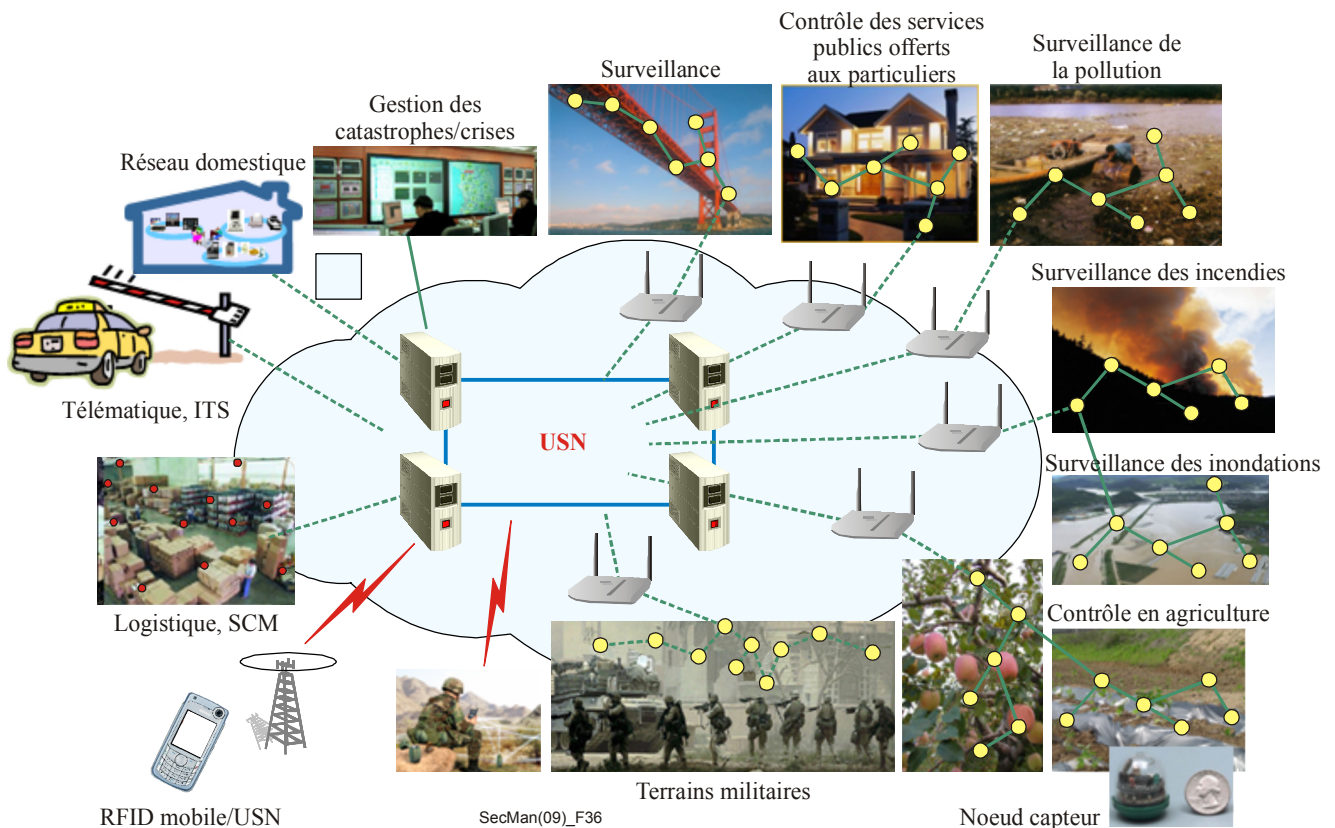


Figure 36 – Applications potentielles des réseaux USN

Les réseaux de capteurs sont généralement raccordés aux réseaux des utilisateurs finals. Même si les réseaux de transmission centraux ont tendance à utiliser les technologies Internet et NGN, diverses technologies sous-jacentes (DSL, satellite, GPRS, CDMA, GSM, etc.) seront utilisées.

Etant donné que le transfert d'informations dans un réseau USN est exposé à de nombreuses menaces potentielles, des techniques de sécurité efficaces sont nécessaires pour lutter contre ces menaces.

En plus des menaces standards qui pèsent sur les réseaux (telles que celles qui sont examinées dans le chapitre 3), certaines menaces pèsent spécifiquement sur les réseaux USN. On peut citer:

- **la compromission de nœuds capteurs**, en raison de l'attaque ou de la compromission de capteurs individuels ou en raison de l'introduction par un attaquant de capteurs illicites;
- **l'écoute clandestine**, par la surveillance des transmissions entre les nœuds;
- **la compromission ou l'exposition de données captées**;
- **les attaques par déni de service** contre les capteurs ou les communications; et
- **l'utilisation malveillante ou abusive de capteurs de réseaux**, par exemple l'utilisation de capteurs à des fins illégales.

De plus, les réseaux USN sont exposés à un certain nombre de menaces liées au routage entre les nœuds capteurs.

Les caractéristiques d'un réseau de capteurs compliquent nettement le processus de conception sécurisée du réseau. Par exemple, en raison de la puissance de traitement et de la mémoire limitées des nœuds capteurs ainsi que de la puissance et de la largeur de bande limitées, il est impossible d'utiliser un chiffrement à clé publique ou de stocker des clés uniques dans les nœuds. De plus, les capteurs peuvent être situés dans des environnements hostiles et il est possible que leur emplacement exact ne soit pas connu après leur déploiement. Enfin, le réseau de capteurs dépend fortement de sa station de base, qui est non seulement un point de défaillance unique potentiel mais aussi une cible tentante pour les attaquants potentiels.

Les intergiciels USN constituent une plateforme d'application commune pour la prise en charge de diverses fonctions pour le compte d'applications et de services USN et pour commander les réseaux de capteurs. Le grand volume de données collectées par le réseau de capteurs est stocké, géré et analysé par les intergiciels USN, qui doivent aussi acheminer les données en toute sécurité aux applications appropriées. Les mesures de sécurité des intergiciels doivent prendre en compte la sécurité des données lorsqu'elles sont stockées et lorsqu'elles sont transmises ainsi que la disponibilité des intergiciels.

Aucune Recommandation sur les réseaux USN n'a encore été finalisée, mais les travaux sont bien engagés pour ce qui est de la prise en compte des besoins de sécurité des réseaux USN proprement dits et de ceux des intergiciels USN.

9. Sécurité des applications

9 Sécurité des applications

De plus en plus conscients de l'importance de la sécurité, les développeurs d'application font aujourd'hui davantage attention à la nécessité d'intégrer la sécurité dans leurs produits, plutôt que d'essayer de mettre en œuvre la sécurité après coup au stade de la production. Malgré cela, des vulnérabilités intrinsèques sont découvertes dans la plupart des applications, à un moment ou à un autre de leur cycle de vie. De plus, l'évolution des menaces a souvent pour effet d'exposer des vulnérabilités auparavant inconnues qui sont alors exploitées.

Dans ce chapitre, on examine les fonctionnalités de sécurité d'un certain nombre d'applications des TIC, en mettant l'accent sur les fonctionnalités de sécurité définies dans les Recommandations UIT-T.

9.1 Téléphonie IP (VoIP) et multimédia

La téléphonie IP, également appelée voix sur IP (VoIP, *voice-over-IP*), désigne la fourniture de services traditionnellement offerts par le réseau téléphonique public commuté (RTPC) à commutation de circuit via un réseau utilisant le protocole Internet (IP). Parmi ces services figurent essentiellement les communications téléphoniques, mais aussi d'autres formes de média, y compris la vidéo et les données. La téléphonie IP inclut aussi les services complémentaires associés tels que les conférences (par pont de conférence), le renvoi d'appel, l'appel en instance, les lignes multiples, la déviation d'appel, la mise en garde et l'interception d'appel, la consultation et la fonction "suis-moi", et bien d'autres services de réseau intelligent. La téléphonie sur Internet est un cas particulier de VoIP, dans lequel le trafic téléphonique est acheminé sur l'Internet public.

La Recommandation UIT-T H.323, *Systèmes de communication multimédia en mode paquet*, est une Recommandation cadre qui jette les bases des communications audio, vidéo et de données sur les réseaux à commutation par paquets, y compris l'Internet, les réseaux locaux (LAN, *local-area network*) et les réseaux étendus (WAN, *wide-area network*), qui n'offrent pas de qualité de service garantie. Ces réseaux, qui sont actuellement les principaux réseaux utilisés dans les entreprises, emploient les technologies de réseau suivantes: TCP/IP à commutation par paquets et échange de paquets Internet (IPX) sur Ethernet, Fast Ethernet et Token Ring. Les produits et applications multimédias issus de différents fabricants mais conformes à la Rec. UIT-T H.323 peuvent interfonctionner, ce qui permet aux utilisateurs de communiquer sans avoir à se soucier de la compatibilité. Le protocole UIT-T H.323 a été le premier protocole de téléphonie IP à être défini et il est considéré comme la pierre angulaire pour les produits fondés sur la téléphonie IP destinés aux applications de divertissement ou professionnelles des particuliers, des entreprises et des fournisseurs de services. Les spécifications de sécurité pour la série de Recommandations UIT-T H.323 sont énoncées dans les Recommandations UIT-T H.Imp235, *Implementors Guide for ITU-T H.235 V3: "Security and encryption for H-series (ITU-T H.323 and other ITU-T H.245-based) multimedia terminals"*, UIT-T H.235.x, série de neuf cadres et normes de sécurité et UIT-T H.530, *Procédures de sécurité symétrique pour la mobilité des systèmes H.323 selon la Recommandation H.510*. La mobilité pour systèmes et services multimédias UIT-T H.323 fait l'objet de la Rec. UIT-T H.510.

La Rec. UIT-T H.323, au domaine d'application vaste, inclut les dispositifs autonomes et les ordinateurs personnels intégrés ainsi que les communications point à point et multipoint.

La Rec. UIT-T H.323 définit quatre principaux composants pour un système de communication fondé sur le réseau: terminaux, passerelles, portiers et ponts de conférence. En outre, des éléments frontières ou homologues sont également possibles. Ces éléments apparaissent sur la Figure 37.

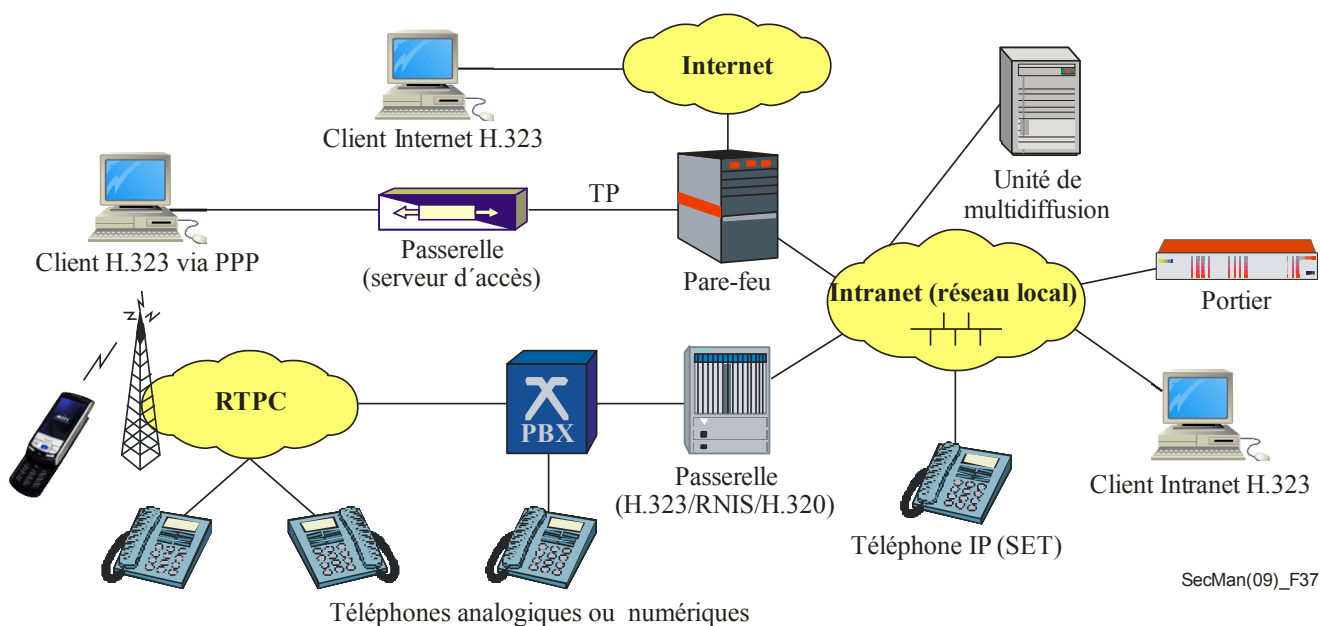


Figure 37 – Système H.323: composants et scénarios de déploiement

Le protocole UIT-T H.323 est par exemple utilisé pour le transit en masse par les opérateurs, notamment dans les réseaux dorsaux de téléphonie IP et pour les services de carte d'appel. Dans les entreprises, le protocole UIT-T H.323 est utilisé pour les autocommutateurs IP, les centrex IP, les réseaux privés virtuels téléphoniques, les systèmes téléphonie et données intégrées, les téléphones Wi-Fi, l'implémentation de centres d'appel et les services de mobilité. A titre professionnel, les personnes l'utilisent largement pour les conférences téléphoniques (ou audio) et vidéo, pour la collaboration téléphonie/données/vidéo et pour la formation à distance. A titre privé, elles l'emploient notamment pour l'accès audiovisuel à large bande et pour les communications de PC à téléphone, de téléphone à PC ou de PC à PC; le protocole H.323 peut aussi être utilisé pour la diffusion d'informations et d'actualités personnalisées.

9.1.1 Problèmes de sécurité dans le domaine du multimédia et de la téléphonie IP

Comme tous les éléments d'un système UIT-T H.323 peuvent être répartis géographiquement et que les réseaux IP sont ouverts, il existe plusieurs menaces de sécurité, comme l'illustre la Figure 38.

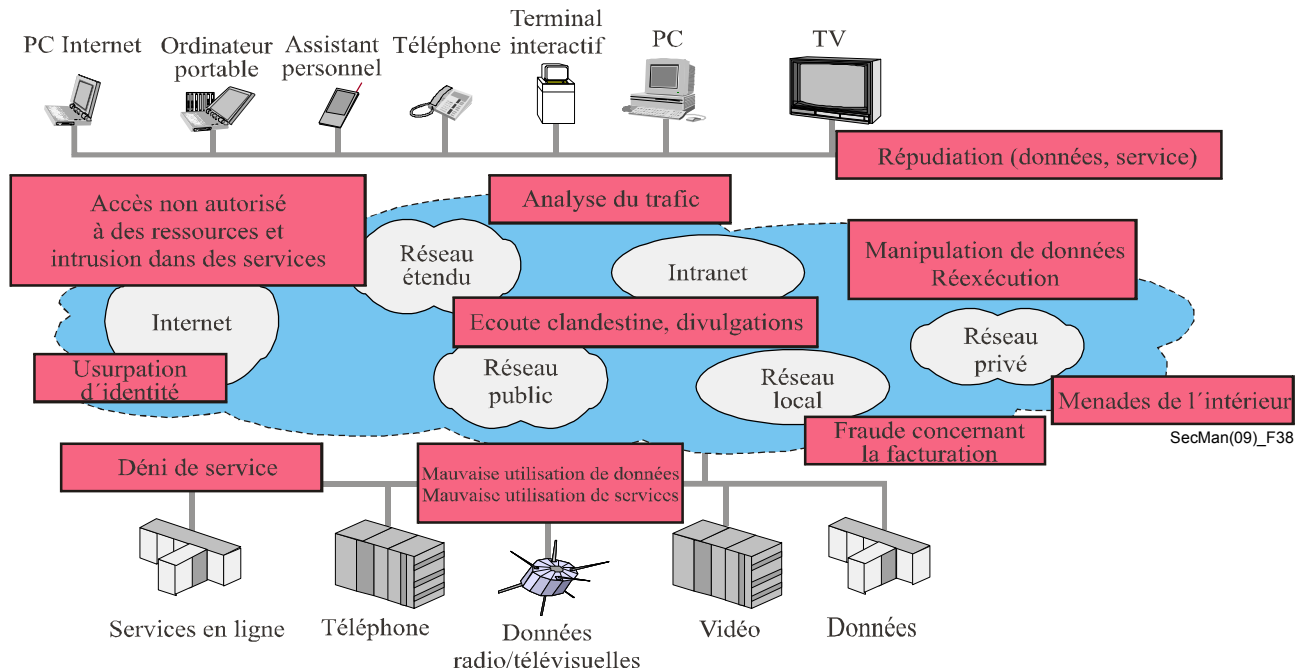


Figure 38 – Menaces de sécurité dans les communications multimédias

Les principaux aspects liés à la sécurité des communications multimédias et de la téléphonie IP sont les suivants:

- **Authentification d'utilisateur et de terminal:** les fournisseurs de service de téléphonie IP ont besoin de savoir qui utilise leur service pour pouvoir comptabiliser et éventuellement facturer correctement l'utilisation du service. En vue de l'authentification, l'utilisateur et/ou le terminal doit d'abord s'identifier, puis prouver que l'identité déclarée est la véritable identité. Pour cela, il est généralement fait appel à des procédures d'authentification forte par chiffrement (par exemple mot de passe protégé ou signatures numériques UIT-T X.509).
- **Authentification de serveur:** comme les utilisateurs de téléphonie IP communiquent généralement entre eux par le biais d'une certaine infrastructure de téléphonie IP faisant intervenir des serveurs (portiers, unités de multidiffusion, passerelles), ils ont besoin de savoir s'ils sont reliés au serveur correct et/ou au fournisseur de service correct. Ceci s'applique tant aux utilisateurs fixes qu'aux utilisateurs mobiles.
- **Authentification d'utilisateur/de terminal et de serveur:** elle est nécessaire pour lutter contre les menaces de sécurité, telles que l'usurpation d'identité, les attaques de l'intercepteur, l'usurpation d'adresse IP et le détournement de connexion.
- **Autorisation d'appel:** il s'agit du processus qui consiste à déterminer si l'utilisateur/le terminal est réellement autorisé à utiliser une fonctionnalité de service (appel dans le RTPC, etc.) ou une ressource de réseau (qualité de service, largeur de bande, codec etc.). Le plus souvent, les fonctions d'authentification et d'autorisation sont utilisées ensemble pour prendre une décision au niveau du contrôle d'accès. L'authentification et l'autorisation aident à contrecarrer les attaques de type usurpation d'identité, utilisation abusive et fraude, manipulation et déni de service.
- **Protection de sécurité de la signalisation:** il s'agit de protéger les protocoles de signalisation contre les manipulations et les utilisations abusives et d'assurer la confidentialité et le respect de la vie privée. Pour protéger les protocoles de signalisation, on utilise généralement le chiffrement et des mesures de protection de l'intégrité et de protection contre les réexecutions. Il faut tout

particulièrement veiller à ce que les facteurs de qualité critiques des communications en temps réel soient respectés afin d'éviter toute dégradation de service due au traitement de la sécurité.

- Confidentialité téléphonique: réalisée par le chiffrement des paquets téléphoniques, elle assure la protection contre les écoutes clandestines. En général, les paquets de média (par exemple vidéo) d'applications multimédias sont chiffrés tout comme les données vocales. La protection renforcée des paquets de média comprend également l'authentification/la protection d'intégrité des charges utiles.
- Gestion de clés: elle inclut non seulement toutes les tâches qui sont nécessaires pour que les informations relatives aux clés puissent être distribuées de manière sécurisée aux utilisateurs et aux serveurs, mais aussi des tâches telles que la mise à jour de clé en cas d'expiration et le remplacement des clés perdues. La gestion de clés peut être exécutée en dehors de l'application de téléphonie IP (configuration de mot de passe) ou peut être intégrée à la signalisation lorsque des profils de sécurité avec capacités de sécurité sont négociés dynamiquement et que des clés de session doivent être distribuées.
- Sécurité interdomaines: elle prend en compte le problème qui se pose lorsque des systèmes appartenant à des environnements hétérogènes ont mis en œuvre des fonctionnalités de sécurité différentes en raison de besoins différents, de politiques de sécurité différentes et de capacités de sécurité différentes. Il faut donc négocier dynamiquement des profils et des capacités de sécurité tels que des algorithmes de chiffrement et leurs paramètres. Cela devient particulièrement important lorsque des frontières entre domaines sont franchies et lorsque des fournisseurs et des réseaux différents interviennent. En ce qui concerne les communications interdomaines, il est important, du point de vue de la sécurité, de pouvoir traverser les pare-feu sans encombre et de pouvoir faire face aux contraintes liées aux traducteurs d'adresse de réseau (NAT, *network address translation*).

Cette liste n'est pas complète mais il s'agit là de l'essentiel de la sécurité UIT-T H.323. Parmi les aspects liés à la sécurité qui sont considérés comme ne faisant pas partie du domaine d'application UIT-T H.323, on peut citer la politique de sécurité, la sécurité de gestion de réseau, la configuration de la sécurité, la sécurité de mise en œuvre, la sécurité opérationnelle et la prise en charge des incidents de sécurité.

9.1.2 Aperçu des Recommandations de la sous-série H.235.x

La série de Recommandations H.235.x comprend onze normes et un guide de mise en œuvre qui, ensemble, spécifient des mécanismes et protocoles de sécurité et donnent des indications détaillées sur la mise en œuvre de la sécurité dans la série de Recommandations UIT-T H.323. Elle décrit des solutions de sécurité modulables pour des petits groupes, des entreprises et des exploitants de grande envergure et permet d'assurer la protection cryptographique des protocoles de commande et des données de flux médias audio/vidéo.

La série UIT-T H.235 offre des moyens permettant de négocier les services cryptographiques, les algorithmes de chiffrement et les capacités de sécurité requis. Les fonctions de gestion de clés pour l'établissement de clés de session dynamiques sont entièrement intégrées aux procédures de prise de contact, ce qui permet de réduire la durée d'établissement d'appel. Les configurations prises en charge comprennent la configuration point à point "classique" et les configurations multipoint avec unités de multidiffusion dans lesquelles plusieurs terminaux multimédias communiquent dans un groupe.

La série UIT-T H.235 utilise des techniques de sécurité optimisées particulières (cryptographie à courbe elliptique et chiffrement AES par exemple) afin de respecter les contraintes strictes de qualité. Lorsque le chiffrement téléphonique est mis en œuvre, on procède au chiffrement des charges utiles RTP dans la couche application. Cette façon de procéder est avantageuse; en effet, elle a peu d'incidence sur les points d'extrémité grâce à une interaction étroite avec le processeur de signaux numériques et les codecs de compression vocale et elle ne dépend pas d'une plate-forme de système d'exploitation particulière.

La Figure 39 illustre le domaine d'application de la série UIT-T H.235, qui contient des dispositions relatives à l'établissement d'appels (blocs UIT-T H.225.0 et UIT-T H.245) et de communications bidirectionnelles

(chiffrement de charges utiles RTP contenant des signaux audio et/ou vidéo compressés). Les fonctionnalités comprennent des mécanismes pour l'authentification, l'intégrité, le respect de la vie privée et la non-répudiation. Les portiers sont chargés de l'authentification lors du contrôle de l'admission au niveau des points d'extrémité et de fournir des mécanismes de non-répudiation. La sécurité dans la couche de transport et dans les couches inférieures, fondée sur IP, sort du cadre des Recommandations UIT-T H.323 et UIT-T H.235, mais elle est couramment mise en œuvre au moyen des protocoles de sécurité IP (IPSec) et de sécurité dans la couche transport (TLS, *transport layer security*). Lorsque la politique du système d'extrémité l'exige, le protocole IPSec ou TLS peut être utilisé pour assurer l'authentification et, facultativement, la confidentialité dans la couche IP quel que soit le protocole (d'application) qui est exécuté au-dessus.

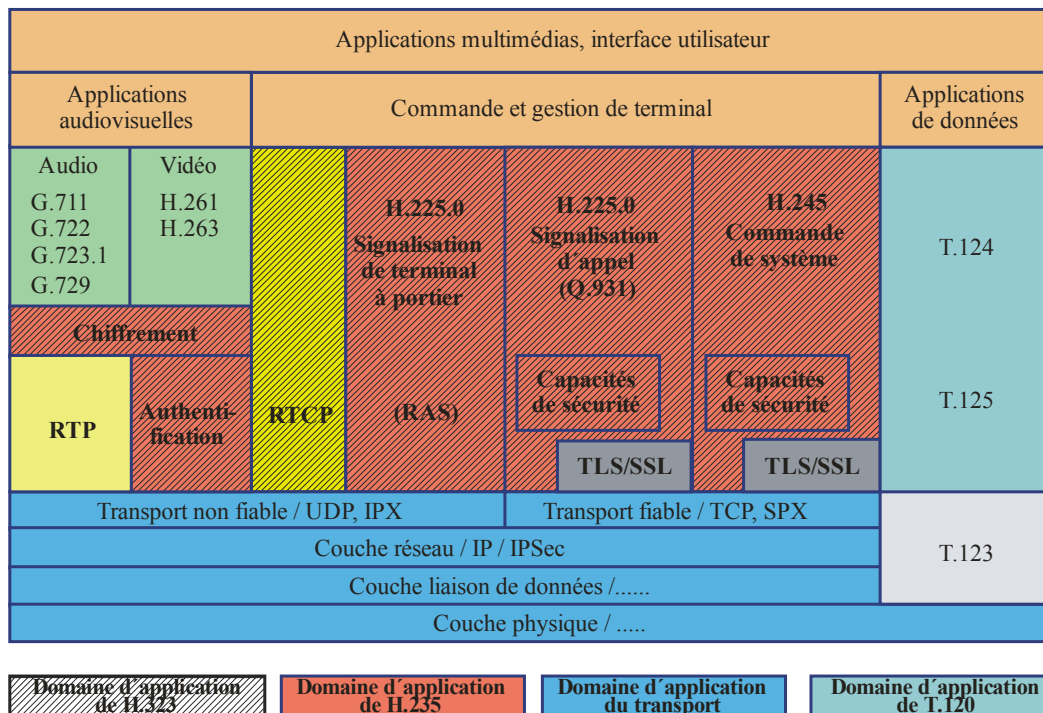


Figure 39 – Sécurité des systèmes UIT-T H.323 offerte par la série UIT-T H.235

Les Recommandations UIT-T de la série UIT-T H.235.x décrivent une large palette de mesures de sécurité qui sont applicables dans différents environnements cibles (par exemple les environnements intra/inter-entreprises et les environnements d'opérateurs) et qui peuvent être adaptées aux besoins et propres à un scénario, suivant des facteurs locaux tels que l'infrastructure de sécurité disponible et les capacités de terminal (par exemple points d'extrémité simples ou points d'extrémité intelligents).

Les profils de sécurité disponibles vont de simples profils à secret partagé avec mot de passe protégé à des profils plus complexes avec signatures numériques et certificats PKI UIT-T X.509 (UIT-T H.235.2). Ainsi, il est possible de mettre en œuvre une protection bond par bond en utilisant les techniques les plus simples mais les moins modulables ou une protection de bout en bout en utilisant les techniques PKI modulables. La Rec. UIT-T H.235.3 est appelée profil de sécurité hybride car elle combine les procédures de sécurité symétriques de la Rec. UIT-T H.235.1 avec les signatures et certificats fondés sur l'infrastructure PKI et les signatures de la Rec. UIT-T H.235.2, ce qui permet d'optimiser la performance et de raccourcir les temps d'établissement d'appel. La Rec. UIT-T H.235.4 assouplit la nécessité stricte d'une architecture centrée sur un serveur et avec routage par portier et définit des mesures de sécurité visant à sécuriser un modèle d'homologue à homologue. Elle définit en outre des procédures de gestion de clé dans des environnements d'entreprise et dans des environnements interdomaines.

Afin d'assurer une plus grande sécurité des systèmes qui utilisent des numéros d'identification personnels (PIN, *personal identification number*) ou des mots de passe pour authentifier les utilisateurs, la Rec. UIT-T H.235.5 définit un "cadre de l'authentification sécurisée pendant l'échange de messages RAS au moyen de secrets partagés faibles" fondé sur l'utilisation de méthodes à clé publique pour sécuriser l'utilisation des numéros PIN/mots de passe. La Rec. UIT-T H.235.6, *Profil pour le chiffrement vocal avec gestion de clés native dans les systèmes H.235/H.245*, rassemble toutes les procédures qui sont nécessaires pour le chiffrement du flux de médias RTP, y compris la gestion de clés associée qui est entièrement exprimée dans les champs de signalisation UIT-T H.245.

La mobilité des utilisateurs et des terminaux en toute sécurité dans des environnements UIT-T H.323 répartis fait l'objet de la Rec. UIT-T H.530, *Procédures de sécurité symétrique pour la mobilité des systèmes H.323 selon la Recommandation H.510*, qui aborde notamment les aspects de sécurité suivants:

- authentification et autorisation d'utilisateur/de terminal mobile dans des domaines visités à l'étranger;
- authentification du domaine visité;
- gestion de clés sécurisée; et
- protection des données de signalisation entre un terminal mobile et un domaine visité.

La Rec. UIT-T H.235.0 décrit le cadre général de sécurité pour les systèmes multimédias de la série H. La Rec. UIT-T H.235.0 et les Rec. UIT-T de la série H.350 définissent une gestion de clés modulable fondée sur le protocole rapide d'accès à l'annuaire (LDAP, *lightweight directory access protocol*) et la couche de connecteurs sécurisés (SSL/TLS, *secure socket layer*). En particulier, la série UIT-T H.350 définit des capacités qui permettent aux entreprises et aux opérateurs de gérer en toute sécurité de très nombreux utilisateurs de services de vidéo et téléphonie IP et permet de relier les protocoles UIT-T H.323, SIP, UIT-T H.320 et les services de messagerie génériques à un service d'annuaire, de manière à ce que les pratiques modernes de gestion d'identité puissent être appliquées aux communications multimédias.

9.1.3 Traducteurs d'adresse de réseau et pare-feu

L'Internet a été conçu suivant le principe "de bout en bout". Autrement dit, deux dispositifs quelconques raccordés au réseau peuvent communiquer directement entre eux. Toutefois, en raison de préoccupations liées à la sécurité et d'un manque d'adresses de réseau IPv4, des pare-feu (FW) et des traducteurs d'adresse de réseau (NAT) sont souvent employés à la frontière des réseaux. Ces frontières entourent le domaine de la résidence, le domaine du fournisseur de services, le domaine de l'entreprise et quelquefois le domaine du pays. Parfois, plusieurs pare-feu ou dispositifs NAT sont employés dans un même domaine. Les pare-feu sont conçus pour contrôler le passage des informations à travers les frontières de réseau et sont généralement configurés pour bloquer la plupart des communications IP. Si un pare-feu n'est pas configuré explicitement pour laisser passer le trafic UIT-T H.323 provenant de dispositifs externes afin que ce trafic aboutisse aux dispositifs UIT-T H.323 internes, la communication est tout simplement impossible, ce qui pose problème pour tout utilisateur d'équipement UIT-T H.323.

Les traducteurs NAT traduisent les adresses utilisées dans le domaine interne en adresses utilisées dans le domaine externe et inversement. Les adresses utilisées dans un domaine résidentiel ou dans un domaine d'entreprise sont généralement, mais pas toujours, attribuées à partir des espaces d'adresses de réseau privé définis dans la norme IETF RFC 1918, qui sont les suivants:

Classe	Intervalle d'adresses	Nombre d'adresses IP
A	10.0.0.0 – 10.255.255.255	16 777 215
B	172.16.0.0 – 172.31.255.255	1 048 575
C	192.168.0.0 – 192.168.255.255	65 535

Les dispositifs NAT posent un problème encore plus frustrant pour la plupart des protocoles IP, en particulier ceux qui acheminent des adresses IP dans le protocole. Les protocoles UIT-T H.323, SIP et d'autres protocoles de communication en temps réel qui fonctionnent sur des réseaux à commutation par paquets doivent fournir des informations de port et d'adresse IP de sorte que les autres participants à la communication sachent où envoyer les flux de média (par exemple flux audio et vidéo).

Les questions relatives à la traversée des dispositifs NAT/FW sont abordées dans trois des Recommandations de la série UIT-T H.460, qui permettent aux communications UIT-T H.323 de traverser de façon transparente un ou plusieurs dispositifs NAT/FW. Il s'agit des Recommandations UIT-T H.460.17, *Utilisation de la connexion de signalisation d'appel H.225.0 pour le transport de messages RAS H.323*, UIT-T H.460.18, *Traversée de traducteurs d'adresse de réseau et de pare-feu par des flux de signalisation H.323* et UIT-T H.460.19, *Traversée de traducteurs d'adresse de réseau et de pare-feu par des flux de média H.323*.

La Figure 40 montre comment un "proxy" spécial pourrait être utilisé pour permettre aux flux provenant de dispositifs "non compatibles" NAT/FW de traverser facilement et correctement les dispositifs NAT/FW:

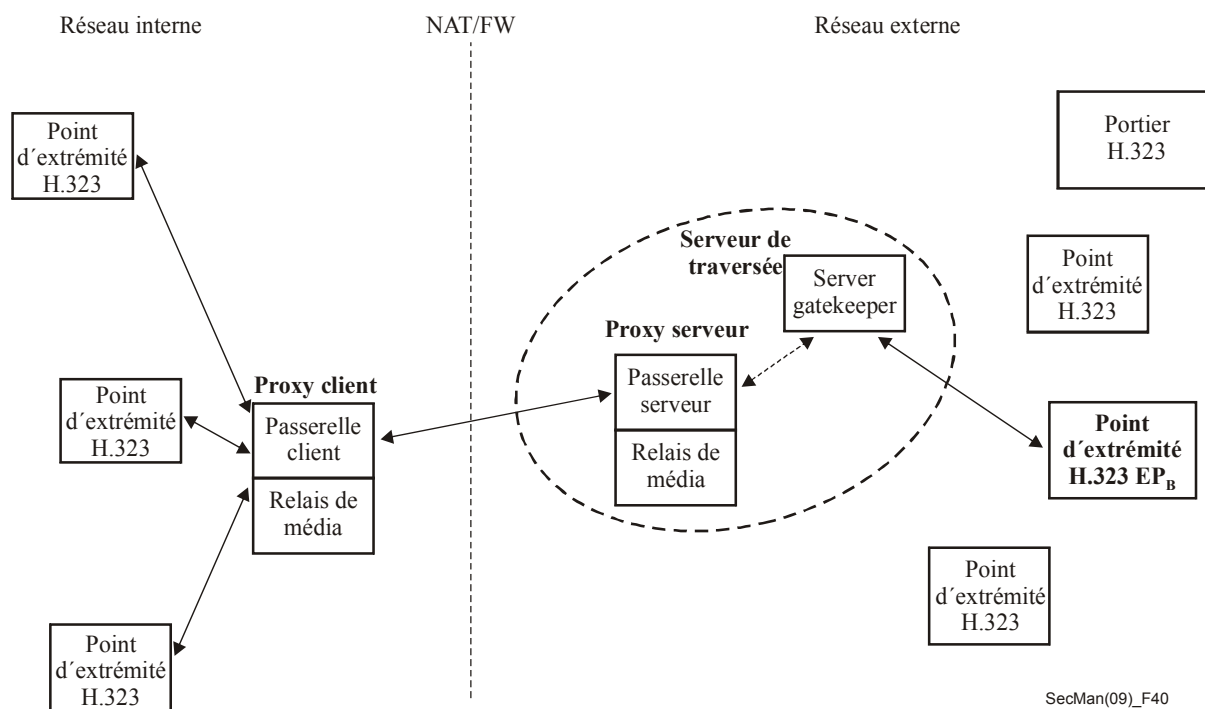


Figure 40 – Traversée de dispositifs NAT/FW dans l'architecture H.460.18

La topologie ci-dessus peut par exemple être utilisée lorsqu'une entreprise souhaite contrôler la route que les flux de signalisation d'appel et de média UIT-T H.323 empruntent dans le réseau. Toutefois, les Rec. UIT-T H.460.17 et H.460.18 permettent aussi aux flux provenant de points d'extrémité de traverser les dispositifs NAT/FW sans l'aide d'un "proxy" interne spécial. La Figure 41 illustre la topologie correspondante:

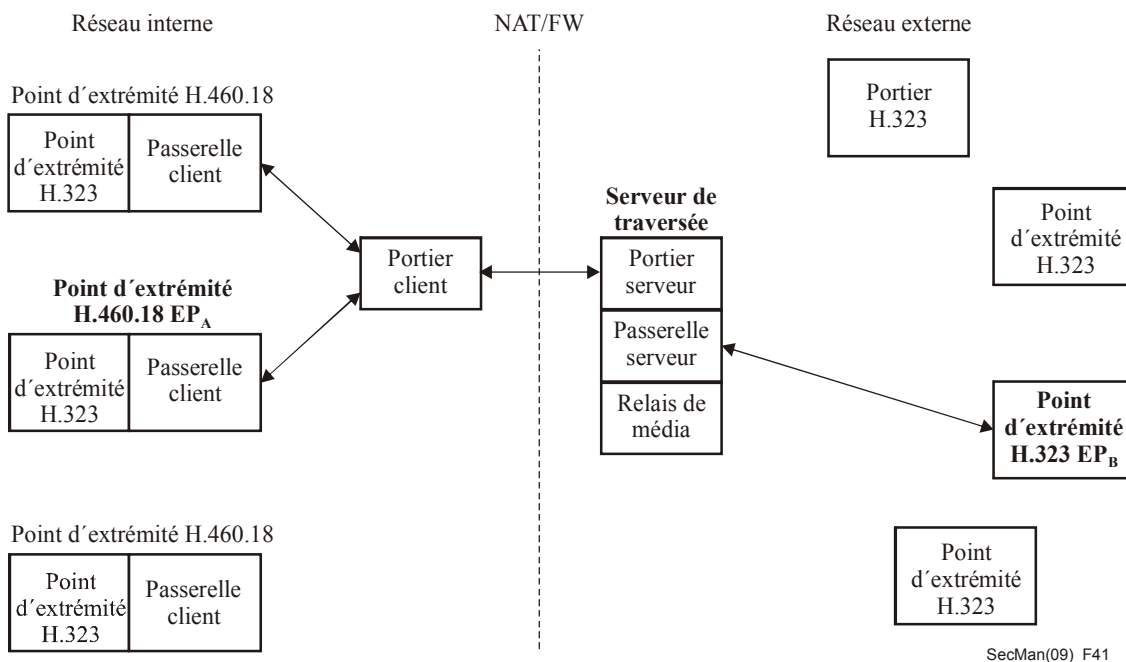


Figure 41 – Architecture avec communication entre portiers

Sur la Figure 41, les points d'extrémité du réseau interne communiquent avec le portier du réseau interne pour résoudre l'adresse des entités externes (par exemple une adresse IP obtenue à partir d'un numéro de téléphone ou d'une adresse URL UIT-T H.323). Le portier du réseau interne communique avec un portier du réseau externe pour échanger ces informations d'adressage et achemine ces informations au point d'extrémité appelant. Lorsqu'un dispositif situé dans le réseau interne lance un appel à destination d'un dispositif situé dans le réseau externe, il utilisera les procédures UIT-T H.460.18 pour ouvrir les "microtrous" nécessaires dans les dispositifs NAT/FW pour laisser passer la signalisation du réseau interne au réseau externe. Il utilisera en outre les procédures UIT-T H.460.19 pour ouvrir les "microtrous" nécessaires pour permettre aux flux de médias de passer correctement du réseau interne au réseau externe et inversement.

Lorsque les dispositifs appelant et appelé résident dans des réseaux privés différents séparés par des dispositifs NAT/FW et l'Internet public, au moins une "passerelle serveur" et un "relais de média" (définis dans la Rec. UIT-T H.460.18) sont nécessaires pour pouvoir acheminer correctement la signalisation et les médias entre les deux réseaux privés. Cette combinaison de dispositifs est généralement appelée "contrôleur de limite de session". La raison en est simple: par conception, un paquet IP provenant d'un réseau privé ne peut pénétrer dans un autre réseau privé qu'avec l'aide d'une entité ("proxy") du réseau public.

9.2 TVIP

Les dispositions prises pour la sécurité de la télévision par protocole Internet (TVIP) doivent permettre de protéger les contenus acheminés par le biais des services de TVIP, les dispositifs terminaux utilisés et la fourniture de ces services.

La protection de contenu de TVIP consiste à faire en sorte qu'un utilisateur final ne puisse utiliser le contenu qu'en fonction des droits que lui a octroyés le titulaire des droits. Il s'agit notamment de protéger les contenus contre la copie et la distribution illégales, l'interception, la falsification et l'utilisation non autorisée.

La protection de dispositif terminal de TVIP consiste à faire en sorte que le dispositif dont se sert un utilisateur final pour recevoir un service puisse utiliser en toute sécurité et fiabilité le contenu, les droits

d'utilisation du contenu étant respectés et l'intégrité et la confidentialité du contenu et des paramètres de sécurité essentiels tels que les clés cryptographiques étant protégées.

La protection de service de TVIP consiste à faire en sorte que les utilisateurs finals puissent uniquement acquérir un service et le contenu qu'ils sont habilités à recevoir. Il s'agit notamment de protéger le service contre tout accès non autorisé.

La Rec. UIT-T X.1191, *Spécifications fonctionnelles et architecture concernant les aspects de sécurité de la TVIP*, a été approuvée et un certain nombre d'autres Recommandations portant spécifiquement sur la sécurité de la TVIP sont en cours d'élaboration. L'architecture générale de sécurité de la TVIP définie dans la Rec. UIT-T X.1191 est représentée sur la Figure 42. Il est à noter que seules les fonctions qui s'appliquent à l'utilisateur final, au fournisseur de réseau et au fournisseur de service sont considérées comme faisant partie du domaine d'application de la Recommandation. Les fonctions se rapportant au fournisseur de contenu font l'objet d'accords privés entre les parties prenantes et sont considérées comme ne faisant pas partie du domaine d'application de cette Recommandation.

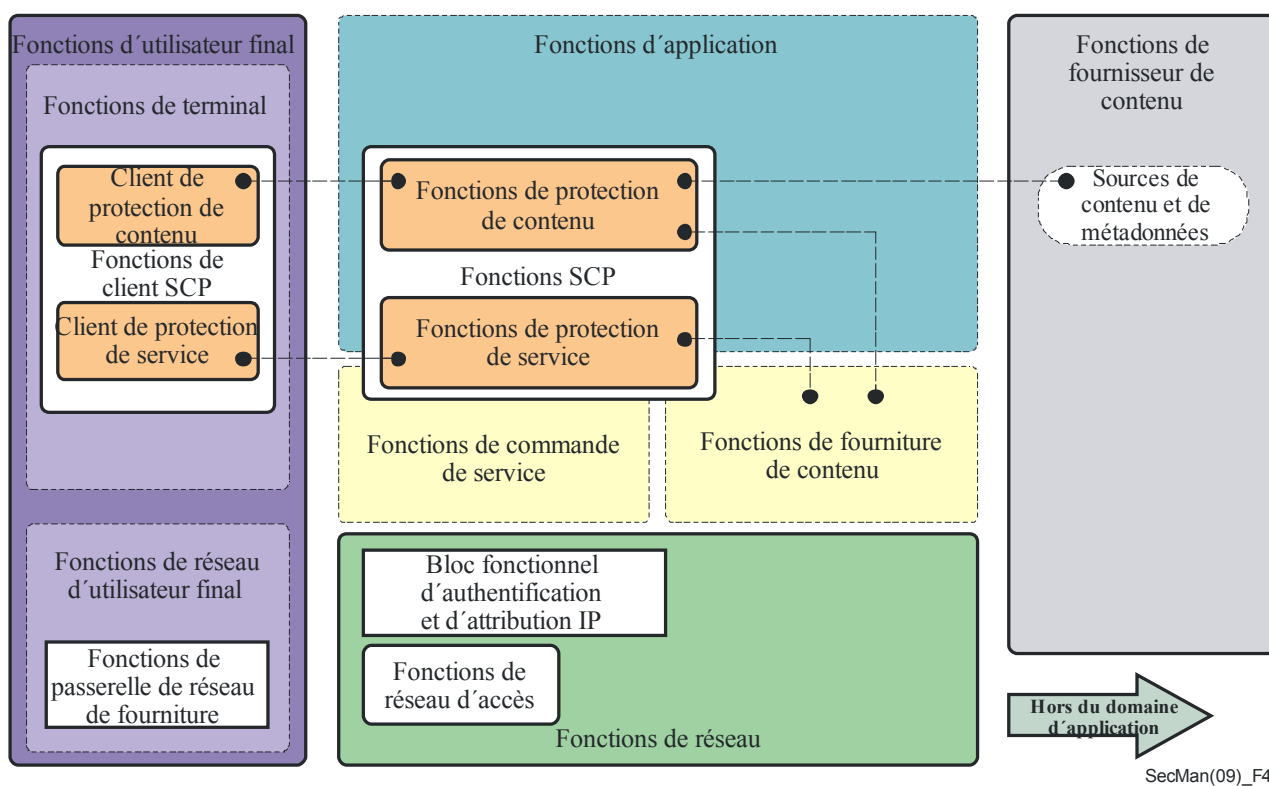


Figure 42 – Architecture générale de sécurité pour la TVIP

9.2.1 Mécanismes de protection de contenu de TVIP

Les mécanismes de sécurité qui peuvent être utilisés pour protéger un contenu sont notamment les suivants:

- chiffrement du contenu;
- filigrane (c'est-à-dire l'utilisation de la stéganographie pour modifier certaines caractéristiques du contenu sans que cette modification puisse être détectée facilement);
- identification et informations de traçage de contenu afin de faciliter les investigations en cas d'accès non autorisé à un contenu ou d'utilisation non autorisée d'un contenu;
- étiquetage du contenu (par exemple avec des informations de notation pour permettre aux utilisateurs finals d'avoir un certain contrôle sur l'accès à un contenu approprié); et

- transcodage sécurisé (qui permet aux nœuds de réseau intermédiaires de changer le format ou la qualité d'un contenu multimédia sans déchiffrement, d'où une préservation de la sécurité de bout en bout).

9.2.2 Mécanismes de protection de service de TVIP

Les mécanismes de protection de service sont notamment les suivants:

- authentification de l'utilisateur final (abonné) et/ou du dispositif terminal;
- autorisation (pour s'assurer que l'utilisateur final ou le terminal est autorisé à accéder aux services et/ou au contenu); et
- contrôle d'accès (tout particulièrement pour faire en sorte que seul un fournisseur de service autorisé puisse accéder au contenu qui est téléchargé d'un client vers un serveur).

9.2.3 Protection des informations d'abonné

Lors de la mise en œuvre de la TVIP, il faut bien prendre en compte la nécessité de protéger les informations d'abonné qui peuvent inclure des données qui sont suivies comme le numéro de chaîne avant et après un changement de chaîne, l'heure du changement, des informations d'utilisateur pour le service de guide de programmes électronique, l'identification du paquetage, l'heure de lecture, etc. Ces données doivent être considérées comme sensibles et des mesures doivent être prises pour éviter toute divulgation non autorisée via le terminal, le réseau ou le fournisseur de service. Des suggestions pour protéger les informations d'abonné sont formulées dans une annexe à la Rec. UIT-T X.1191.

9.3 Transmission de télécopie sécurisée

La télécopie reste une application courante mais la confiance dans les services de télécopie dépend fortement de l'efficacité des mesures de sécurité intégrées. Au départ, les normes de télécopie ont été élaborées pour une transmission sur le RTPC (Rec. UIT-T T.4) puis pour une transmission sur le RNIS (Rec. UIT-T T.563). Plus récemment, des extensions ont été spécifiées pour la transmission de télécopie en temps réel sur les réseaux IP (y compris l'Internet) (Rec. UIT-T T.38) et via des systèmes avec stockage et retransmission (Rec. UIT-T T.37).

Quel que soit le mode de transmission, les problèmes de sécurité affectant les services de télécopie concernent la confidentialité des données transmises, l'authentification et la non-répudiation. Ces problèmes sont devenus d'autant plus importants que le trafic s'est déplacé sur l'Internet, en raison du caractère ouvert et réparti du support.

La sécurité de la transmission de télécopie fait l'objet de la Rec. UIT-T T.36, *Capacités de sécurité à utiliser avec les télécopieurs du Groupe 3*, qui définit deux solutions techniques indépendantes pouvant être utilisées pour le chiffrement des documents échangés. L'une des solutions consiste à utiliser l'algorithme de chiffrement de *Rivest, Shamir & Adleman* (RSA) tandis que l'autre consiste à utiliser une combinaison de *Hawthorne Key Management* (HKM) et de *Hawthorne Facsimile Cipher* (HFX). Les services de sécurité définis sont les suivants:

- authentification mutuelle (obligatoire);
- service de sécurité (optionnel) incluant l'authentification mutuelle, l'intégrité des messages et la confirmation de réception des messages;
- service de sécurité (optionnel) incluant l'authentification mutuelle, la confidentialité des messages (chiffrement) et l'établissement de clé de session; et
- service de sécurité (optionnel) incluant l'authentification mutuelle, l'intégrité des messages, la confirmation de réception des messages, la confidentialité des messages (chiffrement) et l'établissement de clé de session.

La combinaison des systèmes HKM et HFX offre les capacités de sécurité suivantes concernant les communications de document entre entités:

- authentification d'entité mutuelle;
- établissement de clé de session secrète;
- confidentialité de document;
- confirmation de réception; et
- confirmation ou réfutation d'intégrité de document.

9.4 Services web

Les technologies web, en particulier les architectures orientées service (SOA, *service-oriented architecture*), sont largement utilisées car elles permettent de développer et de déployer de nouveaux services de façon efficace et peu onéreuse, et d'intégrer des contenus provenant de diverses sources pour former des services composites facilement et rapidement. Les aspects de sécurité des services web sont nombreux. Les mécanismes d'authentification et de connexion unique (SSO, *single sign-on*) sont importants. Etant donné que les services web sont utilisés dans les réseaux mobiles, il est également important de tenir compte des mécanismes de sécurité nécessaires pour les services web mobiles.

Les économies d'échelle ont conduit les fabricants de plateformes informatiques à développer des produits ayant des fonctionnalités très générales, de sorte qu'ils puissent être utilisés dans la plus large gamme possible de situations. Ces produits sont fournis avec le maximum possible de privilèges concernant l'accès aux données et l'exécution des logiciels, de sorte qu'ils puissent être utilisés dans le plus grand nombre possible d'environnements d'application, y compris ceux qui ont les politiques de sécurité les plus permissives. Lorsqu'une politique de sécurité plus restrictive est requise, les privilèges intrinsèques à la plateforme doivent être restreints, par une configuration locale.

La politique de sécurité d'une grande entreprise comporte de nombreux éléments et de nombreux points d'application. Les éléments de la politique peuvent être gérés par le département des systèmes d'information, par les ressources humaines, par le département des affaires juridiques et par le département des finances. La politique peut être appliquée via l'extranet, le courrier, le réseau étendu et les systèmes d'accès à distance, plateformes qui par nature mettent en œuvre une politique de sécurité permissive. La pratique actuelle consiste à gérer la configuration de chaque point d'application de façon indépendante afin de mettre en œuvre la politique de sécurité de façon aussi précise que possible. Par conséquent, modifier la politique de sécurité est une proposition coûteuse et non fiable. Il est également difficile (voire impossible) d'obtenir une vue d'ensemble des garanties effectives à travers toute l'entreprise pour l'application de la politique. En même temps, il y a une pression croissante sur la direction de l'entreprise, de la part des clients, des actionnaires et des régulateurs pour qu'elle fasse la preuve qu'elle protège le mieux possible le capital d'informations de l'entreprise et de ses clients.

Pour ces raisons, un langage commun est nécessaire pour exprimer la politique de sécurité. S'il est mis en œuvre dans l'ensemble d'une entreprise, un langage de politique commun permet à l'entreprise de gérer l'application de tous les éléments de sa politique de sécurité dans tous les composants de ses systèmes d'information. La gestion de la politique de sécurité peut inclure tout ou partie des étapes suivantes: rédaction, révision, test, approbation, publication, combinaison, analyse, modification, retrait, consultation et application de la politique.

En outre, un cadre est nécessaire pour les échanges d'informations de sécurité. Pour faciliter ces échanges, des langages de balisage ont été élaborés, dont le langage de balisage d'assertion de sécurité et le langage de balisage extensible de contrôle d'accès (XACML, *eXtensible Access Control Markup Language*). Elaborés au départ par OASIS, ces langages ont ensuite été adoptés et publiés par l'UIT-T avec l'assistance d'OASIS.

9.4.1 Langage de balisage d'assertion de sécurité

La Recommandation UIT-T X.1141 définit le langage de balisage d'assertion de sécurité (SAML 2.0). SAML est un cadre fondé sur XML pour l'échange d'informations de sécurité. Ces informations de sécurité sont exprimées sous la forme d'assertions sur des sujets, où un sujet est une entité qui a une identité dans un certain domaine de sécurité. Une même assertion peut contenir plusieurs déclarations internes différentes concernant l'authentification, l'autorisation et les attributs.

Les assertions SAML sont habituellement faites à propos d'un *sujet*. En principe, un certain nombre de *fournisseurs de service* peuvent utiliser des assertions sur un sujet afin de contrôler l'accès et fournir un service personnalisé, et en conséquence, ils deviennent les consommateurs d'assertions d'un producteur d'assertions appelé *fournisseur d'identité*.

La Rec. UIT-T X.1141 définit trois différentes sortes de déclarations d'assertion qui peuvent être créées par une autorité SAML. Toutes les déclarations définies en SAML sont associées à un sujet. Les trois sortes de déclaration définies dans la Rec. UIT-T X.1141 sont:

- authentification: le sujet de l'assertion a été authentifié par un moyen particulier à un moment précis;
- attribut: le sujet de l'assertion est associé aux attributs fournis;
- décision d'autorisation: une demande d'autorisation du sujet de l'assertion à accéder aux ressources spécifiées a été accordée ou refusée.

La Rec. UIT-T X.1141 définit également un protocole par lequel les clients peuvent demander des assertions à des autorités SAML et obtenir d'elles une réponse. Ce protocole, qui consiste en formats de messages de demande et de réponse fondés sur XML, peut être lié à de nombreux protocoles sous-jacents de communication et de transport différents. En créant leurs réponses, les autorités SAML peuvent utiliser diverses sources d'information, comme des mémoires de politique externes et des assertions reçues en entrée dans des demandes.

Un ensemble de profils est défini pour prendre en charge la connexion unique (SSO, *single sign-on*) des navigateurs et autres dispositifs des clients. La Figure 43 illustre le schéma de base pour la réalisation de SSO.

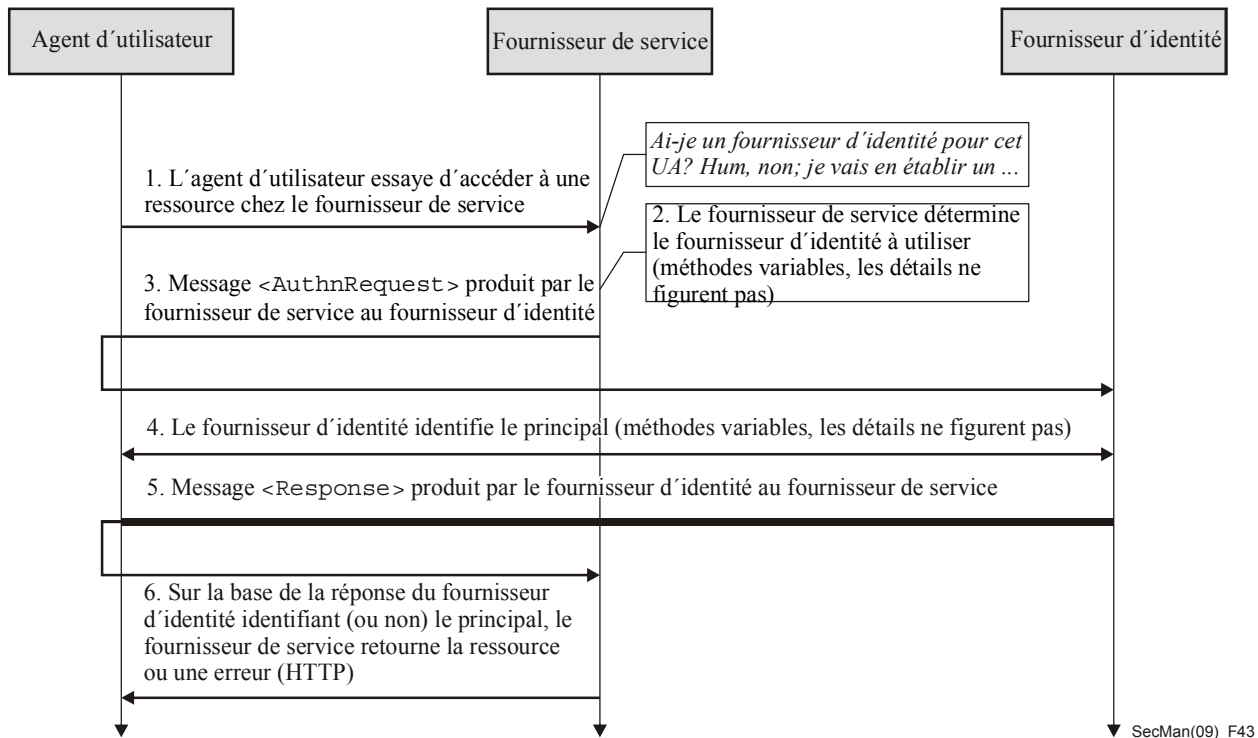


Figure 43 – Schéma de base pour la réalisation de SSO

9.4.2 Langage de balisage extensible de contrôle d'accès

Le langage de balisage extensible de contrôle d'accès (XACML, *eXtensible Access Control Markup Language*) est un vocabulaire XML pour exprimer les politiques de contrôle d'accès. Le contrôle d'accès consiste à décider si l'accès demandé à une ressource devrait être admis et à mettre en application cette décision. La Recommandation UIT-T X.1142 définit le cœur de XACML, y compris la syntaxe du langage, les modèles, le contexte avec le modèle de langage de politique, les règles de syntaxe et de traitement. Pour améliorer la sécurité des échanges de politiques fondées sur XACML, la Rec. UIT-T X.1142 spécifie aussi un profil de signature numérique XML de XACML pour sécuriser les données. Un profil de confidentialité est spécifié afin de fournir des lignes directrices pour l'implémentation. XACML est adapté à divers environnements d'application.

9.5 Services par étiquette

Les étiquettes d'identification (notamment les étiquettes RFID) sont largement utilisées mais les préoccupations sont de plus en plus grandes quant au risque d'atteinte à la vie privée. Ceci s'explique en partie par le fait que la technologie RFID permet de collecter et de traiter automatiquement des données et qu'il existe un risque de divulgation délibérée ou accidentelle d'informations sensibles et/ou personnelles.

S'agissant des applications qui utilisent l'identification par étiquette et qui font intervenir des informations personnelles (soins de santé, passeports, permis de conduire, etc.), la question de la confidentialité pose des problèmes de plus en plus graves.

Au niveau des universités et de l'industrie, la plupart des efforts pour élaborer des mécanismes de protection des informations d'identification personnelle (PII, *personally identifiable information*) ont porté sur l'élaboration de protocoles d'authentification entre l'étiquette ID et le terminal ID. Toutefois, ces efforts ne permettent pas de résoudre complètement les problèmes car des informations utiles relatives à l'identificateur

existent toujours sur le serveur dans le domaine du réseau. Une solution consiste à utiliser un mécanisme de protection des informations PII qui soit fonction du profil.

La Recommandation UIT-T X.1171, *Menaces et protection requise pour les informations d'identification personnelle dans les applications utilisant l'identification par étiquette*, examine les menaces qui pèsent sur les informations PII dans un environnement entreprise-client (B2C, *business-to-customer*) dans lequel les applications utilisent l'identification par étiquette. Elle énonce les spécifications de protection des informations PII dans un tel environnement et définit la structure de base de la protection des informations PII basée sur un profil de politiques PII définies par l'utilisateur.

Les applications B2C utilisant l'identification par étiquette peuvent se classer en trois types, comme suit:

- a) *L'utilisateur du dispositif est le client*: Dans le service de fourniture de contenu d'informations, le client extrait les informations au moyen de son dispositif de lecture. Dans ce type de service, la plupart des fournisseurs de service d'application peuvent supposer que le client a un terminal mobile doté d'un dispositif de lecture. La Figure 44 montre un modèle de base de ce type d'application, se composant de deux opérations de base sur le réseau: la résolution ID et l'extraction du contenu. La résolution ID est la procédure consistant à traduire ou à "réduire" un identificateur en une adresse. Le terminal mobile doté d'un dispositif de lecture commence par réduire un identificateur, qu'il a reçu en provenance de l'étiquette ID via le service d'annuaire, avant d'exécuter une opération d'extraction du contenu.

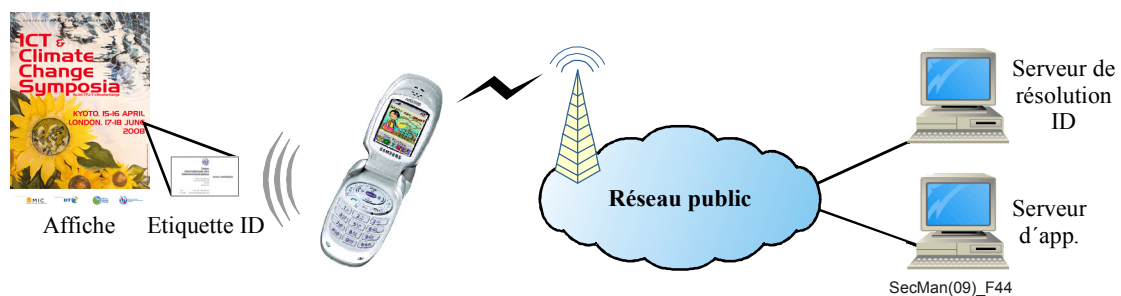


Figure 44 – Modèle de base d'une application B2C utilisant l'identification par étiquette

- b) *L'utilisateur de l'étiquette ID est le client*: Un exemple type de cette application B2C utilisant l'identification par étiquette concerne le contrôle d'accès et/ou l'authentification, par exemple le contrôle des entrées, les passeports, les permis ou le service de gestion après-vente. Dans ce type d'application, les dispositifs de lecture sont des terminaux fixes et/ou des terminaux mobiles. Le client n'a pas besoin de posséder son propre dispositif de lecture.
- c) *Le client est à la fois utilisateur de l'étiquette ID et du dispositif*: Dans le service d'extraction des informations relatives à des produits, le client devient aussi utilisateur de l'étiquette dès qu'il achète le produit étiqueté après avoir lu les informations relatives au produit avec son terminal mobile. Un autre exemple peut être un service dans le domaine des soins de santé déclenché par une carte de patient dotée d'une étiquette ID. Dans cette application, de nombreux types de "clients" peuvent utiliser l'étiquette ID (par exemple le patient, le médecin, l'infirmière). L'utilisateur de l'étiquette ID peut consulter son propre dossier médical grâce au terminal mobile doté d'un dispositif de lecture en lisant sa carte de patient qui est dotée d'une étiquette ID.

Pour les applications B2C qui utilisent l'identification par étiquette, il existe deux principaux risques d'atteinte aux informations PII:

- **Divulgaration d'informations associées à l'identificateur**: Dans ce cas, le pirate peut lire des informations de l'étiquette ID sans qu'en soit conscient l'utilisateur du produit étiqueté. D'abord, le pirate lit un identificateur émis par l'étiquette ID que porte l'utilisateur; ensuite, il réduit

l'identificateur et demande au service d'annuaire la localisation des informations; enfin, il demande des informations associées à l'étiquette ID.

- Divulgarion des données relatives au contexte historique: Le pirate peut extraire des données sur l'utilisateur (préférences, habitudes, centres d'intérêt, etc.), des données relatives au contexte historique associées à l'étiquette ID. Il peut utiliser ce type de données à des fins illicites ou commerciales sans l'accord de l'utilisateur.

La Rec. UIT-T X.1171 décrit les spécifications techniques suivantes afin de protéger les informations PII dans des applications B2C:

- *Gestion des informations PII par l'utilisateur d'étiquette ID:* L'utilisateur d'étiquette ID doit être à même de gérer ou d'actualiser les informations PII associées à son étiquette ID sur le réseau. Il peut ainsi déterminer quelles informations PII devraient être supprimées ou conservées dans l'application.
- *Authentification pour un utilisateur d'étiquette ID et/ou un utilisateur de dispositif:* Le serveur d'application est tenu d'offrir une procédure d'authentification de l'utilisateur d'étiquette ID, et il peut au besoin offrir une procédure d'authentification de l'utilisateur du dispositif (certaines applications utilisant l'identification par étiquette n'ont pas à authentifier l'utilisateur).
- *Contrôle d'accès aux informations PII d'un utilisateur d'étiquette ID dans un serveur d'application:* Le serveur d'application est tenu de contrôler l'accès aux informations PII de l'utilisateur d'étiquette ID.
- *Confidentialité des informations associées à une étiquette ID:* Le serveur d'application est tenu d'assurer la confidentialité des données pour faire en sorte que les informations associées à une étiquette ID ne puissent pas être lues par des utilisateurs non autorisés.
- *Accord en vue de la collecte de données de journalisation relatives à l'utilisateur du dispositif:* Le serveur d'application peut offrir une procédure d'accord pour la collecte de données de journalisation relatives à l'utilisateur du dispositif si ce type de collecte est nécessaire pour l'application.

L'exemple qui suit illustre un service de protection des informations PII (PPS) basé sur le profil de politiques PII de l'utilisateur. Le scénario de service pour le PPS correspond en général à une procédure de personnalisation par étiquette, comme dans le cas de l'achat d'un produit étiqueté. La Figure 45 illustre le flux PPS général pour l'application utilisant l'identification par étiquette.

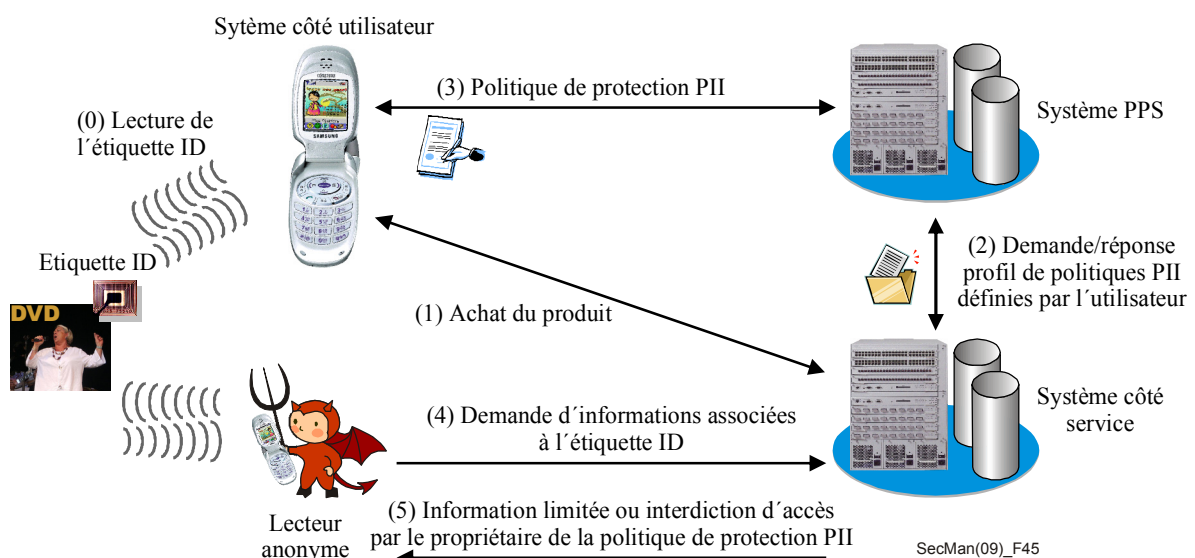


Figure 45 – Flux PPS général

- 0) Un consommateur lit l'identificateur du produit étiqueté à l'aide de son terminal mobile équipé d'un lecteur.
- 1) Le consommateur consulte les informations sur le produit à partir du réseau de services d'application, puis achète le produit en utilisant l'une des diverses méthodes de paiement. A ce moment, le consommateur devient l'utilisateur de l'étiquette ID.
- 2) L'application utilisant l'identification par étiquette demande ensuite au système PPS de lui fournir le profil de politiques PII définies par l'utilisateur, le système fournissant alors à l'application le profil PII en question.
- 3) Le système PPS reçoit la politique de protection des informations PII de l'utilisateur pour cette application.
- 4) N'importe qui peut demander au système côté service les informations associées à cette étiquette ID.
- 5) Le demandeur peut consulter toutes les informations fournies par le système côté service s'il est l'utilisateur de l'étiquette ID. Sinon, soit le demandeur ne peut pas accéder à une quelconque information, soit il obtient des informations limitées.

10. Lutte contre les menaces courantes dans les réseaux

10 Lutte contre les menaces courantes dans les réseaux

Les menaces qui pèsent sur les systèmes informatiques et sur les réseaux qui les interconnectent sont nombreuses et variées. De nombreuses attaques peuvent être déclenchées localement, mais aujourd'hui, la grande majorité des attaques sont réalisées via des réseaux de communications. Le fait que les ordinateurs et les dispositifs de réseau soient toujours plus nombreux à être raccordés à l'Internet et à être utilisés depuis le domicile et depuis le lieu de travail par des personnes peu formées ou peu informées concernant la sécurité informatique augmente considérablement la facilité et la probabilité des attaques distantes, souvent aveugles. Les spams, les logiciels espions, les virus et autres vecteurs d'attaques sont diffusés en nombres de plus en plus grands. Les attaquants profitent souvent de la faiblesse ou de la protection insuffisante des systèmes pour diffuser leurs logiciels malveillants.

Le présent chapitre donne un aperçu des travaux menés par l'UIT-T pour lutter contre certaines de ces menaces.

10.1 Lutte contre le spam

Il est largement admis que le spam (c'est-à-dire le courrier électronique non sollicité) pose un problème considérable aux utilisateurs de réseau et aux fournisseurs de réseau et de service. Le spam interfère avec les communications légitimes, consomme une certaine largeur de bande et des cycles de traitement et, dans les cas extrêmes, peut conduire à des attaques par déni de service résultant de l'inondation des réseaux. Pour lutter contre le spam, on utilise à la fois des mesures juridiques et techniques, avec une efficacité qui varie. Aucune mesure antispam isolée n'est efficace à elle seule et, au vu de l'agilité et de l'ingéniosité des spammeurs, même une combinaison de mesures s'avère souvent efficace uniquement pour ce qui est de réduire le volume de spams. Parmi les mesures utilisées, on peut citer: la réglementation, les mesures techniques (par exemple filtrage du spam), la coopération internationale et la sensibilisation des utilisateurs et des fournisseurs de service Internet.

Les travaux de l'UIT-T sur la lutte contre le spam portent essentiellement sur les aspects techniques du problème. On s'intéresse donc ici aux moyens techniques de lutte contre le spam et à l'élaboration et l'application de technologies antispam.

10.1.1 Stratégies techniques de lutte contre le spam

La Recommandation UIT-T X.1231, *Stratégies techniques de lutte contre le spam*, énonce des spécifications pour lutter contre le spam et sert de point de départ pour les travaux. Elle décrit les différents types de spam et leurs caractéristiques communes et présente les approches techniques pour lutter contre le spam. Elle propose aussi un modèle général qui peut être utilisé pour mettre au point une stratégie antispam efficace.

Ce modèle est un modèle hiérarchique, dans lequel cinq stratégies sont réparties dans trois couches. Les relations entre les stratégies sont illustrées sur la Figure 46. Il ressort de ce modèle que les stratégies dépendent largement les unes des autres mais, dans des cas particuliers, il est possible que les stratégies ne soient pas toutes retenues pour des raisons de coût. De plus, il faut adapter le modèle aux besoins de chaque scénario d'application particulier.

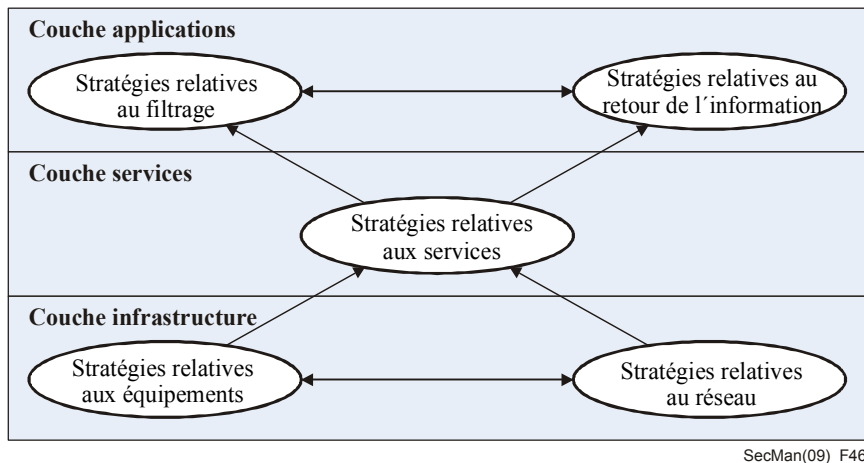


Figure 46 – Modèle général de lutte contre le spam

10.1.2 Spam par courrier électronique

Le spam par courrier électronique est le type de spam le plus répandu. Il pose des difficultés techniques complexes et les solutions mises en œuvre pour en venir à bout doivent s'appuyer sur des mesures techniques appropriées. Si l'intervention de la puissance publique et le rôle de la législation sont utiles, ils ne suffisent pas à répondre aux défis lancés par le spam par courrier électronique. Le problème est d'autant plus complexe qu'il est difficile d'identifier le spammeur lorsque le protocole SMTP est utilisé.

Deux Recommandations ont pour objet de faciliter la lutte contre le spam par courrier électronique. La Rec. UIT-T X.1240, *Technologies intervenant dans la lutte contre le spam par courrier électronique*, s'adresse aux utilisateurs qui souhaitent développer des solutions techniques de lutte contre le spam par courrier électronique. Elle spécifie les concepts fondamentaux, les caractéristiques, les effets et les problèmes techniques associés à la lutte contre le spam par courrier électronique. Elle présente en outre les solutions techniques existantes et les activités connexes réalisées par diverses organisations de normalisation et par d'autres groupes qui travaillent à la lutte contre le spam par courrier électronique.

La Recommandation UIT-T X.1241, *Cadre technique pour lutter contre les spams par courrier électronique*, décrit une structure recommandée d'un domaine de traitement antispam et définit la fonction des principaux modules de ce domaine. Le cadre établit un mécanisme de partage des informations sur les spams par courrier électronique entre les différents serveurs de messagerie électronique. Il vise à promouvoir une plus grande coopération entre les fournisseurs de service dans la lutte contre le spam et, en particulier, à mettre en œuvre une méthode de communication d'alertes lorsqu'un spam est identifié. Un autre document, *Série UIT-T X.1240 - Supplément sur la lutte contre le spam et les menaces associées*, passe en revue les instances internationales qui s'intéressent au spam et contient une étude de cas.

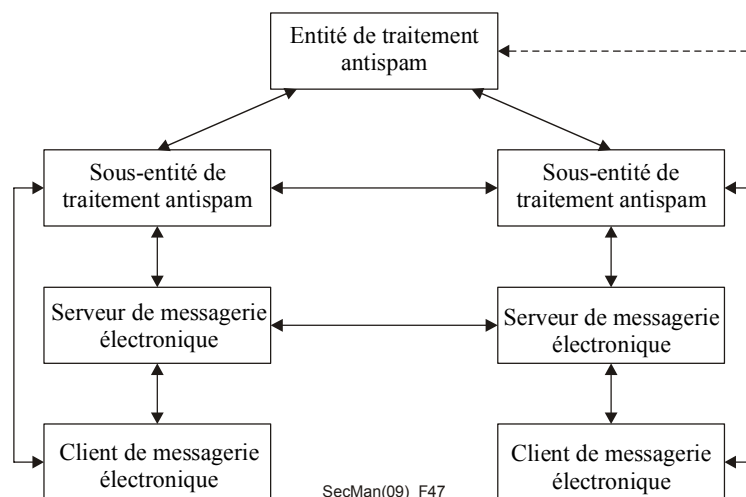


Figure 47 – Structure générale du domaine de traitement antispam applicable au spam par courrier électronique

La Figure 47 illustre les processus du cadre UIT-T X.1241. L'entité de traitement antispam est située dans un système indépendant tandis que les sous-entités de traitement antispam sont situées dans un ou plusieurs fournisseurs de service de messagerie électronique. L'entité de traitement communique de nouvelles règles aux sous-entités, qui doivent les vérifier et les parfaire. Il existe aussi une fonction qui permet de résoudre les éventuels conflits entre les règles.

10.1.3 Spam multimédia IP

La Recommandation UIT-T X.1244, *Aspects généraux de la lutte contre le spam dans les applications multimédias IP*, spécifie les concepts de base, les caractéristiques et les aspects techniques liés à la lutte contre le spam dans les applications multimédias IP (téléphonie IP, messagerie instantanée, etc.). Les divers types de spam d'application multimédia IP sont classés par catégories et leurs caractéristiques sont décrites. La norme décrit diverses menaces de sécurité liées au spam d'application multimédia IP et indique les aspects à prendre en considération pour lutter contre ce type de spam. Parmi les techniques mises au point pour venir à bout du spam de courrier électronique, certaines peuvent aussi être utilisées dans le cas du spam d'application multimédia IP. La Rec. UIT-T X.1244 analyse les mécanismes classiques de lutte contre le spam et examine leur applicabilité dans le cas du spam d'application multimédia IP.

Les techniques antispam peuvent être appliquées au spam multimédia IP en fonction des caractéristiques particulières du spam. Le Tableau 7 illustre la classification utilisée dans la Rec. UIT-T X.1244.

Tableau 7 – Classification des spams d'application multimédia IP

	Texte	Voix	Vidéo
En temps réel	<ul style="list-style-type: none"> spam de messagerie instantanée spam de bavardage 	<ul style="list-style-type: none"> spam de VoIP spam de messagerie instantanée 	<ul style="list-style-type: none"> spam de messagerie instantanée
Pas en temps réel	<ul style="list-style-type: none"> spam de messagerie multimédia/textuelle spam textuel de service de partage de fichier P2P spam textuel de site web 	<ul style="list-style-type: none"> spam de messagerie multimédia/vocale spam vocal de service de partage de fichier P2P spam vocal de site web 	<ul style="list-style-type: none"> spam de messagerie multimédia/vidéo spam vidéo de service de partage de fichier P2P spam vidéo de site web

10.1.4 Spam du service de messages courts (SMS)

La Recommandation UIT-T X.1242, *Système de filtrage des spams du service de messages courts (SMS) basé sur des règles spécifiées par l'utilisateur*, définit la structure et les fonctions du système de filtrage du spam du service SMS, la gestion du service fourni à l'utilisateur, les protocoles de communication et les spécifications fonctionnelles de base des terminaux dotés de fonctions SMS. Elle définit aussi des méthodes permettant aux utilisateurs de gérer (rechercher, supprimer ou restituer) les messages courts filtrés. Le filtrage peut être fondé sur des caractéristiques telles que l'adresse, le numéro de téléphone, l'heure ou le contenu. Les spécifications du logiciel du terminal assurant le filtrage du spam du service SMS sont énoncées dans un appendice à la Rec. UIT-T X.1242.

10.2 Codes malveillants, logiciels espions et logiciels trompeurs

Il est incontestable que ce sont les codes malveillants (virus, vers, chevaux de Troie, etc.) qui présentent le plus de risques pour les systèmes et les réseaux mais les logiciels espions et autres logiciels trompeurs (c'est-à-dire les logiciels qui réalisent des activités non autorisées) présentent également des risques importants. Si les organisations et les individus ne mettent pas en œuvre toute une série de mesures proactives (pare-feu, mesures antivirus, mesures anti-logiciel espion) contre ces menaces, il est presque garanti que leurs systèmes ou réseaux seront compromis. Toutefois, les contremesures disponibles n'ont pas toutes la même efficacité et ne sont pas toujours complémentaires.

Dans de nombreux pays, les régulateurs exigent de plus en plus que les fournisseurs de service fournissent des garanties concernant les mesures de sécurité et de sûreté qu'ils ont prises, et qu'ils aident davantage les utilisateurs à utiliser l'Internet en toute sécurité.

La Recommandation UIT-T X.1207, *Lignes directrices à l'intention des fournisseurs de services de télécommunication pour lutter contre les risques d'installation de logiciels espions ou de tout logiciel potentiellement indésirable*, est une norme visant à:

- a) promouvoir, dans le cadre des services d'hébergement de pages web, les meilleures pratiques fondées sur les principes suivants: obligation d'informer clairement les utilisateurs, nécessité d'obtenir leur consentement et possibilité pour eux d'exercer un contrôle; et
- b) promouvoir les meilleures pratiques (par le biais des fournisseurs de services de télécommunication) à l'intention des particuliers sur l'utilisation sûre et sécurisée des ordinateurs personnels et de l'Internet.

La Rec. UIT-T X.1207 donne aux fournisseurs de service des indications claires sur la gestion des risques de sécurité, l'utilisation de produits sûrs et sécurisés, la surveillance du réseau et les interventions nécessaires, l'assistance, la mise à jour et l'hébergement sécurisé de pages web. Des conseils sont donnés pour guider et sensibiliser les utilisateurs et pour adopter des mesures techniques de protection des utilisateurs finals. Un appendice, qui ne fait pas partie intégrante de la Recommandation, contient des liens vers d'autres ressources.

10.3 Notification et diffusion de mises à jour logicielles

Un code malveillant peut se propager à une rapidité alarmante et, même si des mesures de protection avancées ont été adoptées, de nouvelles menaces peuvent se propager avec une rapidité telle que les systèmes et les réseaux qui ne contiennent pas les dernières mises à jour sont vulnérables. Les systèmes sont également particulièrement vulnérables aux "zero-day exploits" (c'est-à-dire aux menaces nouvelles ou inconnues auparavant pour lesquelles aucune signature antivirus ou aucun correctif n'a encore été élaboré). Dans cet environnement, la distribution et l'installation rapides des mises à jour est essentielle. Toutefois, il existe un certain nombre de problèmes associés à la distribution et à l'installation de ces mises à jour.

La plupart des logiciels du commerce, notamment les systèmes d'exploitation et les systèmes conçus pour assurer une protection de sécurité (antivirus, anti-logiciel espion, pare-feu, etc.), contiennent une fonctionnalité qui permet une mise à jour automatique. Toutefois, cette fonctionnalité doit être activée par l'utilisateur. Lorsqu'un utilisateur est simplement informé du fait que des mises à jour sont disponibles (ou éventuellement du fait que des mises à jour ont été téléchargées), il doit prendre des mesures pour permettre le téléchargement et/ou l'installation de ces mises à jour. De nombreuses mises à jour nécessitent un redémarrage des systèmes après installation, ce que les utilisateurs individuels ne font pas nécessairement immédiatement. Les organisations qui disposent d'un programme de sécurité bien géré procèdent généralement à une gestion centrale des mises à jour et imposent les mises à jour des systèmes des utilisateurs finals. En revanche, la mise à jour des systèmes individuels (par exemple ordinateurs à la maison) et la mise à jour des systèmes dans les petites organisations sont généralement peu méthodiques.

Un autre problème se pose avec les mises à jour: les fournisseurs de logiciels n'utilisent pas de pratiques uniformes pour informer les utilisateurs de la disponibilité de mises à jour ou des conséquences possibles en cas de non-installation des mises à jour. Ils n'utilisent pas non plus de méthode uniforme pour tenir les utilisateurs informés des dernières bonnes pratiques pour préserver la sécurité des logiciels. De plus, il n'existe pas de méthode uniforme pour la notification des problèmes détectés par les utilisateurs après l'installation d'une mise à jour.

La Recommandation UIT-T X.1206, *Cadre indépendant du fournisseur de produits pour la notification automatique d'informations de sécurité et la diffusion automatique de mises à jour*, examine les difficultés rencontrées pour tenir à jour les logiciels et décrit un cadre indépendant du fournisseur pour faire face aux problèmes. Une fois qu'un actif est enregistré, les dernières informations de vulnérabilité et les correctifs ou mises à jour peuvent être diffusés automatiquement aux utilisateurs ou directement dans les applications. La Rec. UIT-T X.1206 définit un cadre que tout fournisseur peut utiliser pour la notification ainsi que pour fournir des informations de vulnérabilité et diffuser les correctifs ou mises à jour nécessaires. Elle définit aussi le format des informations qui devraient être utilisées dans les composants et entre eux.

La Rec. UIT-T X.1206 permet aux administrateurs de système de connaître la situation de tout actif dont ils sont responsables. Elle décrit les problèmes de préservation des actifs du point de vue de leur identification, ainsi que du point de vue de la diffusion des informations et de la gestion des systèmes/du réseau. Elle contient aussi une description de la sécurité qui devrait être prise en considération dans le cadre indépendant du fournisseur.

La Rec. UIT-T X.1206 définit les structures de données des composants qui sont nécessaires pour ces activités, y compris le schéma XML associé, et donne le format des informations qu'il convient d'utiliser dans les composants mettant en œuvre ce cadre et entre eux.

11. L'avenir de la normalisation de la sécurité des TIC

11 L'avenir de la normalisation de la sécurité des TIC

L'UIT-T élabore des normes sur les TIC depuis plus de trente ans. Cette activité s'est nettement accélérée ces dernières années compte tenu de la croissance rapide de l'utilisation de l'Internet et d'autres réseaux et de la nécessité de protéger les utilisateurs et les systèmes contre des menaces de sécurité toujours plus nombreuses et variées.

Le présent manuel a présenté de façon générale certaines initiatives et réalisations essentielles des Commissions d'études de l'UIT-T dans le domaine de la sécurité afin de mieux faire connaître les activités et les difficultés techniques auxquelles les utilisateurs et les implémenteurs de réseau sont confrontés. Les lecteurs sont invités à consulter les nombreuses ressources mises en ligne par l'UIT-T pour obtenir plus de détails sur les aspects présentés ici et à utiliser les Recommandations et les documents d'information afin de contribuer à créer un environnement en ligne plus sûr et d'améliorer la confiance des utilisateurs dans les opérations en ligne.

Si on regarde vers l'avenir, les réseaux de télécommunication et les réseaux informatiques vont continuer à converger. Les réseaux de prochaine génération et les services fondés sur le web vont continuer à croître rapidement et à gagner de l'importance, mais les menaces vont continuer à évoluer. Aussi la conception et l'élaboration de mesures efficaces pour lutter contre ces menaces et la conception et la mise en place de système et de réseaux plus sécurisés de manière à réduire les vulnérabilités intrinsèques resteront-elles des défis.

Les 191 Etats Membres et plus de 551 Membres de Secteur de l'UIT continueront à relever ces défis en continuant à élaborer des Recommandations techniques et des lignes directrices sur la sécurité dans le cadre d'un programme de travail ambitieux dicté par les besoins des membres et guidé par la structure organisationnelle établie à l'Assemblée mondiale de normalisation des télécommunications de 2008. Chaque fois que c'est possible, pour éviter la redondance des tâches et utiliser au mieux les ressources, l'UIT-T collaborera avec d'autres organisations de normalisation pour parvenir à des solutions harmonisées aussi efficacement et rapidement que possible.

12. Sources d'informations complémentaires

12 Sources d'informations complémentaires

Le présent manuel contient un aperçu général des travaux de l'UIT-T sur la sécurité. Des informations beaucoup plus détaillées et de nombreuses normes sont disponibles gratuitement sur le site web de l'UIT-T.

12.1 Aperçu des travaux de la CE 17

Tout d'abord, la page d'accueil de la CE 17 contient des liens vers des informations relatives aux activités de la CE 17 (exposés, résumés de Recommandations en cours d'élaboration, noms des principales personnes). Les liens vers la Commission d'études directrice sur la sécurité des télécommunications et vers la Commission d'études directrice sur la gestion d'identité (IdM) donnent des informations sur les activités et les résultats des travaux de ces deux entités.

12.2 Recueil sur la sécurité

Le recueil contient des informations sur les Recommandations de l'UIT, des informations connexes et des informations sur les activités de l'UIT dans le domaine de la sécurité. Il comprend cinq parties, chacune d'elles pouvant être téléchargée:

- un catalogue des Recommandations approuvées relatives à la sécurité des télécommunications, qui comprend les Recommandations portant expressément sur la sécurité et celles qui décrivent ou utilisent des fonctions utiles pour la sécurité;
- une liste des définitions relatives à la sécurité approuvées par l'UIT-T extraites des Recommandations UIT-T approuvées;
- une présentation succincte des Commissions d'études de l'UIT-T menant des activités dans le domaine de la sécurité;
- une présentation succincte des Recommandations UIT-T faisant l'objet d'un examen relatif aux considérations de sécurité;
- une présentation succincte des autres activités de l'UIT dans le domaine de la sécurité.

12.3 Feuille de route sur les normes de sécurité

La feuille de route sur les normes de sécurité est une ressource en ligne qui donne des informations sur les normes existantes relatives à la sécurité des TIC et les travaux en cours dans les principales organisations de normalisation. En plus des activités de l'UIT-T dans le domaine de la sécurité, la feuille de route contient des informations sur les activités de normalisation de la sécurité menées par l'ISO/CEI, l'ATIS, l'ENISA, l'ETSI, l'IEEE, l'IETF, OASIS, le 3GPP et le 3GPP2.

Comme le recueil, la feuille de route comprend cinq parties et la plupart des informations sont directement accessibles en ligne:

- Partie 1, *Organisations s'occupant de normalisation des TIC et leurs activités*, qui contient des informations sur la structure de la feuille de route et sur chacune des organisations de normalisation répertoriées. La Partie 1 contient aussi des liens vers les glossaires et vocabulaires existants relatifs à la sécurité;
- Partie 2, *Normes approuvées relatives à la sécurité des TIC*, qui contient une base de données des normes de sécurité approuvées avec des liens directs vers la plupart des normes, dans laquelle il est possible de faire des recherches;
- Partie 3, *Normes de sécurité en cours d'élaboration*;
- Partie 4, *Besoins futurs et propositions de nouvelles normes de sécurité*; et

- Partie 5: *Bonnes pratiques en matière de sécurité.*

12.4 Lignes directrices pour la mise en œuvre de la sécurité

Le Supplément 3 à la série de Recommandations UIT-T X.800-X.849, *Lignes directrices pour la mise en œuvre de la sécurité dans les systèmes et dans les réseaux*, contient plus de détails sur certains aspects examinés dans le présent manuel et énonce des lignes directrices pour la mise en œuvre de la sécurité dans les systèmes et dans les réseaux qui peuvent être utilisées pour réaliser un programme de sécurité de réseau. Quatre domaines sont traités: politique de sécurité technique; identification des actifs; menaces, vulnérabilités et solutions pour y remédier; et évaluation de la sécurité. Ce document indique les principaux éléments nécessaires pour établir et gérer la politique technique nécessaire pour gérer les réseaux qui peuvent être exploités par plusieurs opérateurs et qui contiennent des produits et des systèmes provenant de multiples fournisseurs. Il énonce aussi des lignes directrices relatives à des questions réglementaires.

12.5 Informations complémentaires sur l'annuaire, l'authentification et la gestion d'identité

Pour plus d'informations sur les Recommandations de la série UIT-T X.500, la source d'informations faisant autorité est la série de Recommandations UIT-T X.500 proprement dite. On trouvera d'autres informations didactiques et un guide de mise en œuvre à l'adresse: www.x500standard.com. Les liens ci-après donnent des informations complémentaires:

<http://www.x500standard.com/index.php?n=X509.X509ProtectingDirectory> donne des informations sur l'authentification d'utilisateur;

<http://www.x500standard.com/index.php?n=X500.AccessControl> donne plus d'informations sur le contrôle d'accès; et

<http://www.x500standard.com/index.php?n=X500.DataPrivacyProtection> donne une description plus détaillée des fonctionnalités de confidentialité des données X.500.

Annexe A – Définitions relatives à la sécurité

Annexe A

Définitions relatives à la sécurité

Le tableau qui suit contient les définitions des termes employés dans le présent manuel. Toutes les définitions figurent dans les Recommandations UIT-T en vigueur. Une liste plus complète de définitions relatives à la sécurité est contenue dans le recueil des définitions relatives à la sécurité approuvées par l'UIT-T extraites des Recommandations UIT-T tenu à jour par la Commission d'études 17.

Terme	Définition	Référence
contrôle d'accès (<i>access control</i>)	<ol style="list-style-type: none"> 1. Précaution prise contre l'utilisation non autorisée d'une ressource; cela comprend les précautions prises contre l'utilisation d'une ressource de façon non autorisée. 2. Restriction du flux d'informations provenant des ressources d'un système aux personnes, programmes, processus ou autres ressources de système de réseau autorisés. 	<p style="text-align: center;">X.800</p> <p style="text-align: center;">J.170</p>
liste de contrôle d'accès (<i>access control list</i>)	Liste des entités qui sont autorisées à accéder à une ressource, avec leurs autorisations d'accès.	X.800
politique de contrôle d'accès (<i>access control policy</i>)	Ensemble des règles définissant les conditions dans lesquelles l'accès peut se dérouler.	X.812
menaces accidentelles (<i>accidental threats</i>)	Menaces qui existent sans qu'il y ait préméditation. Des exemples de menaces accidentelles qui se sont concrétisées sont: défaillance de système, bévues opérationnelles et bogues dans le logiciel.	X.800
imputabilité (<i>accountability</i>)	Propriété qui garantit que les actions d'une entité ne peuvent être imputées qu'à cette entité.	X.800
algorithme (<i>algorithm</i>)	Processus mathématique qui peut être utilisé pour l'embrouillage et pour le désembrouillage d'un flux de données.	J.93
attaque (<i>attack</i>)	Activités entreprises pour contourner ou exploiter des déficiences constatées dans les mécanismes de sécurité d'un système. Une attaque directe d'un système exploite des déficiences dans les algorithmes, principes ou propriétés sous-tendant un mécanisme de sécurité. Les attaques indirectes consistent à contourner le mécanisme ou à en provoquer une utilisation incorrecte par le système.	H.235
attribut (<i>attribute</i>)	Dans le cadre de la messagerie, élément d'information, composante d'une liste d'attributs, qui décrit un utilisateur ou une liste de distribution et qui peut aussi se rapporter à la structure physique ou organisationnelle du système de messagerie (ou du réseau qui le supporte).	X.400
autorité d'attribut, autorité en charge des attributs (AA, <i>attribute authority</i>)	<ol style="list-style-type: none"> 1. Autorité qui attribue des privilèges par l'émission de certificats d'attribut. 2. Entité bénéficiant de la confiance d'une ou de plusieurs entités pour l'établissement et la signature de certificats d'attribut. <p><i>Note</i> – Une autorité de certification peut également être une autorité en charge des attributs.</p>	<p style="text-align: center;">X.509</p> <p style="text-align: center;">X.842</p>
certificat d'attribut (<i>attribute certificate</i>)	Structure de données, portant la signature numérique d'une autorité d'attribut, qui lie certaines valeurs d'attribut à des informations d'identification concernant son détenteur.	X.509

Terme	Définition	Référence
authentification (<i>authentication</i>)	<ol style="list-style-type: none"> 1. Processus de confirmation d'identité. <i>Note</i> – Voir entité principale (<i>principal</i>) et vérificateur (<i>verifier</i>) et les deux formes d'authentification distinguées (auth. de l'origine des données (<i>data origin auth.</i>) + auth. d'identité (<i>entity auth.</i>)). L'authentification peut être <i>unilatérale</i> ou <i>mutuelle</i>. La première atteste l'identité d'une seule entité principale. La seconde atteste l'identité des deux entités principales. 2. Attestation de l'identité revendiquée par une entité. 3. Voir authentification de l'origine des données (<i>data origin authentication</i>) et authentification de l'entité homologue (<i>peer entity authentication</i>). Le terme authentification n'est pas associé à l'intégrité des données; le terme intégrité des données est utilisé à la place. 4. Corroboration de l'identité des objets se rapportant à l'établissement d'une association. Par exemple, il peut s'agir des entités d'application, des processus d'application et des usagers des applications. <i>Note</i> – Ce terme a été défini en vue d'indiquer clairement qu'il s'agit d'une authentification de portée plus large que l'authentification de l'entité homologue dont traite la Rec. X.800 du CCITT. 5. Processus consistant à vérifier l'identité déclarée d'une entité auprès d'une autre entité. 6. Processus destiné à permettre au système de vérifier avec certitude l'identité d'un tiers. 	<p>X.811</p> <p>X.811 X.800</p> <p>X.217</p> <p>J.170</p> <p>J.93</p>
échange d'authentification, échange pour authentification (<i>authentication exchange</i>)	<ol style="list-style-type: none"> 1. Mécanisme destiné à garantir l'identité d'une entité par échange d'informations. 2. Séquence d'un ou de plusieurs transferts d'informations d'authentification (AI) pour échange, en vue de réaliser une authentification. 	<p>X.800</p> <p>X.811</p>
service d'authentification (<i>authentication service</i>)	Ce service fournit la preuve qu'un objet ou un sujet possède effectivement l'identité qu'il déclare. Les types d'authentification suivants peuvent être nécessaires en fonction du type d'acteur et du but de l'identification: authentification de l'utilisateur, authentification de l'entité homologue, authentification de l'origine des données. Des exemples de mécanismes utilisés pour implémenter le service d'authentification sont l'authentification simple par mot de passe et numéro d'identification personnel (PIN, <i>personal identification number</i>) et l'authentification forte basée sur des méthodes de chiffrement.	M.3016.2
autorité (<i>authority</i>)	Entité responsable de l'émission de certificats. Deux types sont définis: les autorités de certification émettant des certificats de clé publique et les autorités d'attribut émettant des certificats d'attribut.	X.509
autorisation (<i>authorization</i>)	<ol style="list-style-type: none"> 1. Attribution de droits, comprenant la permission d'accès sur la base de droits d'accès. <i>Note</i> – Cette définition implique que les droits sont des droits d'effectuer certaines activités (telles que l'accès aux données) et qu'ils ont été accordés à une entité, un opérateur humain ou un processus. 2. Octroi d'une permission sur la base d'une identité authentifiée. 3. Fait de donner l'accès à un service ou à un dispositif à quelqu'un qui dispose de la permission d'accès. 	<p>X.800</p> <p>H.235</p> <p>J.170</p>
disponibilité (<i>availability</i>)	Propriété d'être accessible et utilisable sur demande par une entité autorisée.	X.800

Terme	Définition	Référence
capacité (<i>capability</i>)	Jeton utilisé comme identificateur d'une ressource de telle sorte que la possession du jeton confère des droits d'accès à cette ressource.	X.800
certificat (<i>certificate</i>)	Ensemble de données relatives à la sécurité, émis par une autorité de sécurité ou par un tiers de confiance en même temps que des informations de sécurité qui sont utilisées pour fournir les services d'intégrité et d'authentification d'origine des données (certificat de sécurité – UIT-T X.810). Ce terme renvoie aux certificats "de clé publique" qui sont des valeurs représentant une clé publique de détenteur (et d'autres informations facultatives), ces valeurs ayant été vérifiées et signées par une autorité de confiance sous une forme infalsifiable.	H.235
politique de certificat (<i>certificate policy</i>)	Ensemble nommé de règles indiquant la possibilité d'appliquer un certificat pour une communauté particulière et/ou une classe d'applications particulière avec des besoins de sécurité communs. Une politique de certificat particulière peut, par exemple, indiquer la possibilité d'application d'un certificat pour des transactions avec échange de données électroniques pour le commerce de biens dans une fourchette de prix donnée.	X.509
liste de révocation de certificats (CRL, <i>certificate revocation list</i>)	<ol style="list-style-type: none"> Liste signée indiquant un ensemble de certificats qui ne sont plus considérés comme valides par leur émetteur. Certains types de listes CRL spécifiques sont définis en plus du type générique de liste CRL, pour couvrir des domaines particuliers. Une liste CRL contient les numéros de série des certificats qui ont été révoqués (par exemple parce que la clé a été compromise ou parce que le sujet ne fait plus partie du personnel) et dont la période de validité n'a pas encore expiré. 	X.509 Q.817
autorité de certification (CA, <i>certification authority</i>)	<ol style="list-style-type: none"> Autorité jouissant de la confiance d'un ou de plusieurs utilisateurs pour la création et l'attribution de certificats. L'autorité de certification peut, de manière optionnelle, créer les clés des utilisateurs. Entité habilitée à laquelle il est fait confiance (dans le contexte d'une politique de sécurité) pour créer des certificats de sécurité contenant une ou plusieurs classes de données relatives à la sécurité. 	X.509 X.810
cryptogramme, texte chiffré (<i>ciphertext</i>)	Données obtenues par l'utilisation du chiffrement. Le contenu sémantique des données résultantes n'est pas compréhensible. NOTE – Le cryptogramme peut lui-même être réinjecté dans un nouveau chiffrement pour produire un cryptogramme surchiffré.	X.800
texte en clair (<i>cleartext</i>)	Données intelligibles dont la sémantique est compréhensible.	X.800
confidentialité (<i>confidentiality</i>)	Propriété d'une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés.	X.800
service de confidentialité (<i>confidentiality service</i>)	Le service de confidentialité fournit une protection contre la divulgation non autorisée de données échangées. On peut distinguer les types de service de confidentialité suivants: confidentialité sélective de champ, confidentialité en mode connexion, confidentialité de flux de données.	M.3016.2
justificatif (<i>credentials</i>)	Données transférées pour établir l'identité déclarée d'une entité.	X.800

Terme	Définition	Référence
analyse cryptographique (<i>cryptanalysis</i>)	<ol style="list-style-type: none"> 1. Analyse d'un système cryptographique, et/ou de ses entrées et sorties, pour en déduire des variables confidentielles et/ou des données sensibles (y compris un texte en clair). 2. Processus consistant à récupérer le texte en clair d'un message ou la clé de chiffrement sans avoir accès à la clé. 3. Science de la récupération du contenu d'un message sans accéder à la clé physique (ou à la clé électronique dans un système cryptographique électronique). 	X.800 J.170 J.93
algorithme cryptographique (<i>cryptographic algorithm</i>)	Fonction mathématique qui calcule un résultat à partir d'une ou de plusieurs valeurs d'entrée.	H.235
système de chiffrement (<i>cryptographic system, cryptosystem</i>)	<ol style="list-style-type: none"> 1. Ensemble de transformations d'un texte en clair pour obtenir un texte chiffré et réciproquement, le choix de la ou des transformations particulières à utiliser se faisant au moyen de clés. Les transformations sont définies en général par un algorithme mathématique. 2. Un système de chiffrement est simplement un algorithme qui peut convertir des données d'entrée en quelque chose de non reconnaissable (chiffrement), et reconvertir ces données non reconnaissables dans leur forme d'origine (déchiffrement). Les techniques de chiffrement RSA sont décrites dans la Rec. UIT-T X.509. 	X.509 Q.815
cryptographie (<i>cryptology</i>)	Discipline incluant les principes, moyens et méthodes de transformation des données, dans le but de cacher leur contenu, d'empêcher que leur modification passe inaperçue et/ou d'empêcher leur utilisation non autorisée. <i>Note</i> – La cryptographie détermine les méthodes de chiffrement et de déchiffrement. Une attaque portant sur les principes, moyens et méthodes de cryptographie est appelée analyse cryptographique.	X.800
confidentialité des données (<i>data confidentiality</i>)	Ce service peut être utilisé pour protéger des données contre une divulgation non autorisée. Le service de confidentialité des données est pris en charge par le cadre d'authentification. Il peut être utilisé pour protéger des données contre les interceptions.	X.509
intégrité des données (<i>data integrity</i>)	Propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée.	X.800
authentification de l'origine des données (<i>data origin authentication</i>)	<ol style="list-style-type: none"> 1. Confirmation que la source des données reçues est telle que déclarée. 2. Corroboration de l'identité de l'entité principale qui est responsable d'une unité de données spécifique. 	X.800 X.811
déchiffrement (<i>decipherment, decryption</i>)	Opération inverse d'un chiffrement réversible.	X.800
délégation (<i>delegation</i>)	Transfert d'un privilège d'une entité détentrice vers une autre entité.	X.509
déni de service (<i>denial of service</i>)	Impossibilité d'accès à des ressources pour des utilisateurs autorisés ou introduction d'un retard pour le traitement d'opérations critiques.	X.800

Terme	Définition	Référence
signature numérique (<i>digital signature</i>)	<ol style="list-style-type: none"> Données ajoutées à une unité de données, ou transformation cryptographique (voir cryptographie (<i>cryptography</i>)) d'une unité de données, permettant à un destinataire de prouver la source et l'intégrité de l'unité de données et protégeant contre la falsification (par le destinataire, par exemple). Transformation cryptographique d'une unité de données qui permet au destinataire de l'unité de données de prouver l'origine et l'intégrité de cette unité de données, qui protège l'émetteur et le destinataire de l'unité de données contre un faux fabriqué par un tiers et qui protège l'émetteur contre un faux fabriqué par le destinataire. 	X.800 X.843
service d'annuaire (<i>directory service</i>)	Service pour la recherche et la récupération d'informations à partir d'un catalogue d'objets bien définis, qui peut contenir des informations sur les certificats, numéros de téléphone, conditions d'accès, adresses, etc. Un exemple en est un service d'annuaire conforme à la Rec. UIT-T X.500.	X.843
écoutes (indiscrètes) (<i>eavesdropping</i>)	Violation de la confidentialité par surveillance de la communication.	M.3016.0
chiffrement (<i>encipherment</i>)	<ol style="list-style-type: none"> Transformation cryptographique (voir cryptographie (<i>cryptography</i>)) de données produisant un cryptogramme. NOTE – Le chiffrement peut être irréversible. Dans ce cas, le déchiffrement correspondant ne peut pas être effectué. Processus consistant à rendre des données illisibles par des entités non autorisées après application d'un algorithme cryptographique (ou de chiffrement). Le déchiffrement est l'opération inverse par laquelle le texte chiffré est transformé en texte clair. 	X.800 H.235
cryptage (<i>encryption</i>)	<ol style="list-style-type: none"> Méthode utilisée pour convertir des informations en clair en cryptogramme. Processus de chiffrement des signaux afin d'éviter un accès non autorisé. 	J.170 J.93
chiffrement de bout en bout (<i>end-to-end encipherment</i>)	Chiffrement de données à l'intérieur ou au niveau du système d'extrémité source, le déchiffrement correspondant ne se produisant qu'à l'intérieur, ou au niveau du système d'extrémité de destination.	X.800
entité (<i>entity</i>)	<ol style="list-style-type: none"> Un être humain, une organisation, une composante de matériel ou un élément de logiciel. Tout élément concret ou abstrait, qui présente un intérêt. Alors que d'une manière générale le terme entité peut être utilisé pour faire référence à toute chose, son utilisation dans le contexte de la modélisation est réservée aux éléments modélisant l'univers du discours. 	X.842 X.902
authentification d'entité (<i>entity authentication</i>)	Corroboration de l'identité d'une entité principale, dans le contexte d'une relation de communication. Note – L'identité authentifiée de cette entité principale n'est garantie que lorsque ce service est invoqué. On peut obtenir la garantie de la continuité d'authentification en suivant la description du 5.2.7/X.811.	X.811
preuve (<i>evidence</i>)	Information qui, par elle-même ou par association avec d'autres informations, peut être utilisée pour résoudre un litige. Note – Formes particulières de preuve: signatures numériques, enveloppes sécurisées et jetons de sécurité. Les signatures numériques sont utilisées avec les techniques de clé publique tandis que les enveloppes sécurisées et les jetons de sécurité sont utilisés avec les techniques de clé privée.	X.813

Terme	Définition	Référence
falsification (<i>forgery</i>)	Une entité crée de toutes pièces des informations dont elle prétend qu'elles ont été reçues d'une autre entité ou émises à destination d'une autre entité.	M.3016.0
fonction de hachage (<i>hash function</i>)	Fonction (mathématique) qui fait correspondre les valeurs d'un grand ensemble (potentiellement très grand) de valeurs à une gamme plus réduite de valeurs.	X.810
attaque indirecte (<i>indirect attack</i>)	Attaque d'un système qui n'est pas fondé sur les déficiences d'un mécanisme de sécurité particulier (par exemple, attaques qui contournent le mécanisme ou qui dépendent de l'utilisation incorrecte du mécanisme par le système).	X.814
intégrité (<i>integrity</i>)	Caractéristique de données qui n'ont pas été altérées de façon non autorisée. (Voir aussi intégrité des données (<i>data integrity</i>).)	H.235
service d'intégrité (<i>integrity service</i>)	Le service d'intégrité fournit des moyens permettant d'assurer que les données échangées sont correctes en fournissant une protection contre la modification, la suppression, la création (insertion) et la répétition des données échangées. On peut distinguer les types de service d'intégrité suivants: intégrité sélective de champ; intégrité de connexion sans reprise; intégrité de connexion avec reprise.	M.3016.2
menaces intentionnelles (<i>intentional threats</i>)	Menaces pouvant aller de l'examen fortuit, utilisant des outils de contrôle facilement disponibles, aux attaques sophistiquées, utilisant une connaissance spéciale du système. Une menace intentionnelle qui se concrétise peut être considérée comme une "attaque".	X.800
IPCablecom	Projet UIT-T comprenant une architecture et une série de Recommandations permettant la fourniture de services en temps réel sur les réseaux de télévision par câble utilisant des câblo-modems.	J.160
Kerberos	Protocole d'authentification de réseau à clé secrète qui utilise plusieurs algorithmes cryptographiques pour le chiffrement et une base de données de clés centralisée pour l'authentification.	J.170
clé (key)	1. Série de symboles commandant les opérations de chiffrement et de déchiffrement. 2. Valeur mathématique introduite dans l'algorithme cryptographique choisi.	X.800 J.170
échange de clés (<i>key exchange</i>)	Echange de clés publiques entre entités à utiliser pour le chiffrement des communications entre ces entités.	J.170
gestion de clés (<i>key management</i>)	Production, stockage, distribution, suppression, archivage et application de clés conformément à une politique de sécurité.	X.800
attaque de l'intercepteur (<i>man-in-the-middle attack</i>)	Attaque dans laquelle un attaquant est en mesure de lire, insérer et modifier à volonté des messages entre deux parties sans qu'aucune des parties ne sache que le lien entre elles a été compromis.	X.1151
usurpation d'identité (<i>masquerade</i>)	Prétention qu'a une entité d'en être une autre.	X.800
authentification mutuelle (<i>mutual authentication</i>)	Attestation de l'identité des deux entités principales.	X.811

Terme	Définition	Référence
non-répudiation (<i>non-repudiation</i>)	<ol style="list-style-type: none"> 1. Capacité d'empêcher à un émetteur de nier ultérieurement avoir envoyé un message ou exécuté une action. 2. Protection contre le déni, par une des entités impliquées dans une communication, d'avoir participé à tout ou partie de celle-ci. 3. Processus par lequel l'expéditeur d'un message (par exemple une demande de paiement à la séance) ne peut pas nier avoir envoyé ce message. 	J.170 H.235 J.93
notarisation (<i>notarization</i>)	Enregistrement de données chez un tiers de confiance permettant de s'assurer ultérieurement de leur exactitude (contenu, origine, date, remise).	X.800
menace passive (<i>passive threat</i>)	Menace d'une divulgation non autorisée des informations, sans que l'état du système ne soit modifié.	X.800
mot de passe (<i>password</i>)	<ol style="list-style-type: none"> 1. Information d'authentification confidentielle, habituellement composée d'une chaîne de caractères. 2. Chaîne de mot de passe saisie par l'utilisateur: il s'agit de la clé de sécurité attribuée que l'utilisateur mobile partage avec son domaine de rattachement. Ce mot de passe de l'utilisateur et le secret partagé de l'utilisateur qui en découle doivent être utilisés aux fins d'authentification de l'utilisateur. 	X.800 H.530
sécurité physique (<i>physical security</i>)	Mesures prises pour assurer la protection des ressources contre des menaces délibérées ou accidentelles.	X.800
entité principale (<i>principal</i>)	Entité dont l'identité peut être authentifiée.	X.811
respect de la vie privée, secret des communications (<i>privacy</i>)	<ol style="list-style-type: none"> 1. Droit des individus de contrôler ou d'agir sur des informations les concernant, qui peuvent être collectées et stockées, et sur les personnes par lesquelles et auxquelles ces informations peuvent être divulguées. <i>Note</i> – Ce terme étant lié au droit privé, il ne peut pas être très précis et son utilisation devrait être évitée sauf pour des besoins de sécurité. 2. Mode de communication dans lequel seules les parties explicitement habilitées peuvent interpréter la communication. Le secret des communications est normalement réalisé par chiffrement et par partage de clé(s) pour accéder au chiffre. 	X.800 H.235
clé privée (<i>private key</i>)	<ol style="list-style-type: none"> 1. (Dans un système de chiffrement avec clé publique) celle des clés d'une paire de clés d'un utilisateur qui est connue uniquement par l'utilisateur concerné. 2. Clé qui est utilisée avec un algorithme asymétrique de cryptographie et dont la possession est limitée (habituellement à une seule entité). 3. Clé utilisée en cryptographie à clé publique qui appartient à une entité individuelle et qui doit être tenue secrète. 	X.509 X.810 J.170
privilège (<i>privilege</i>)	Attribut ou propriété attribué par une autorité à un utilisateur.	X.509
infrastructure de gestion de privilège (PMI, <i>privilege management infrastructure</i>)	Infrastructure qui peut prendre en charge la gestion des privilèges correspondant à un service complet d'autorisation et en relation avec une infrastructure de clé publique.	X.509

Terme	Définition	Référence
clé publique (<i>public key</i>)	<ol style="list-style-type: none"> (Dans un système de chiffrement avec clé publique) celle des clés d'une paire de clés d'un utilisateur qui est connue de manière publique. Clé qui est utilisée avec un algorithme asymétrique de cryptographie et qui peut être rendue publique. Clé utilisée en cryptographie à clé publique qui appartient à une entité individuelle et est distribuée publiquement. Les autres entités utilisent cette clé pour chiffrer les données à envoyer au propriétaire de la clé. 	X.509 X.810 J.170
certificat de clé publique (<i>public key certificate</i>)	<ol style="list-style-type: none"> Clé publique d'un utilisateur, associée à certaines autres informations qui sont rendues non falsifiables par chiffrement en utilisant la clé privée de l'autorité de certification émettrice. Valeurs représentant une clé publique de détenteur (et d'autres informations facultatives), ces valeurs ayant été vérifiées et signées par une autorité de confiance sous une forme infalsifiable. Relation entre la clé publique d'une entité et un ou plusieurs attributs relatifs à son identité, également appelé certificat numérique. 	X.509 H.235 J.170
cryptographie à clé publique (<i>public key cryptography</i>)	<p>Technique cryptographique fondée sur un algorithme à deux clés (publique et privée), dans laquelle un message est chiffré avec la clé publique mais ne peut être déchiffré qu'au moyen de la clé privée. Également appelé système PPK (clé privée-publique).</p> <p>Note – Le fait de connaître la clé publique ne permet pas d'en déduire la clé privée. Par exemple, le correspondant A construit une clé publique et une clé privée de ce type. Il envoie la clé publique sans restriction à tous ceux qui souhaitent communiquer avec lui, mais il garde la clé privée secrète. Tous ceux qui possèdent la clé publique peuvent alors crypter un message pour le correspondant A, mais seul celui-ci peut décrypter ces messages, à l'aide de sa clé privée.</p>	J.93
infrastructure de clé publique (PKI, <i>public key infrastructure</i>)	Infrastructure pouvant prendre en charge la gestion de clés publiques afin de fournir des services d'authentification, de chiffrement, d'intégrité et de non-répudiation.	X.509
partie utilisatrice (<i>relying party</i>)	Utilisateur ou agent qui utilise les données contenues dans un certificat pour prendre des décisions.	X.509
répétition (<i>replay</i>)	Un message ou une partie d'un message est répété pour produire un effet non autorisé. Par exemple, un message valide contenant des informations d'authentification peut être répété par une autre entité pour s'authentifier elle-même (comme quelque chose qu'elle n'est pas).	X.800
répudiation (<i>repudiation</i>)	<ol style="list-style-type: none"> Le fait, pour une des entités impliquées dans la communication, de nier avoir participé aux échanges, totalement ou en partie. Une entité nie son implication dans un échange de communication antérieur. (Dans un système MHS, c'est) quand un utilisateur du système MTS ou le système MTS ont ultérieurement la possibilité de refuser le dépôt, la réception ou l'expédition d'un message. Les risques de répudiation sont les suivants: refus d'origine, refus de dépôt, refus de remise. 	X.800 M.3016.0 X.402
certificat de révocation de liste (<i>revocation list certificate</i>)	Certificat de sécurité qui identifie une liste de certificats de sécurité qui ont été révoqués.	X.810

Terme	Définition	Référence
clé secrète (<i>secret key</i>)	Clé qui est utilisée avec un algorithme symétrique de cryptographie. La possession de cette clé est limitée (habituellement à deux entités).	X.810
sécurité (<i>security</i>)	Le terme " <i>sécurité</i> " est utilisé dans le sens d'une minimisation des vulnérabilités d'actifs et de ressources. Un actif est tout élément de valeur. Une <i>vulnérabilité</i> est toute faiblesse qui pourrait être exploitée pour violer un système ou les informations qu'il contient. Une <i>menace</i> est une violation potentielle de la sécurité.	X.800
alarme de sécurité (<i>security alarm</i>)	Message généré lorsqu'un événement lié à la sécurité, défini par la politique de sécurité comme étant une condition d'alarme, a été détecté. Une alarme de sécurité est destinée à être portée à temps à l'attention d'entités appropriées.	X.816
audit de sécurité (<i>security audit</i>)	Revue indépendante et examen des enregistrements et des activités du système afin de vérifier l'exactitude des contrôles du système pour s'assurer de leur concordance avec la politique de sécurité établie et les procédures d'exploitation, pour détecter les infractions à la sécurité et pour recommander les modifications appropriées des contrôles, de la politique et des procédures.	X.800
journal d'audit de sécurité (<i>security audit trail</i>)	Données collectées et pouvant éventuellement être utilisées pour permettre un audit de sécurité.	X.800
certificat de sécurité (<i>security certificate</i>)	Ensemble de données relatives à la sécurité émis par une autorité de sécurité ou une tierce partie de confiance ainsi que les informations de sécurité qui sont utilisées pour fournir des services d'intégrité et d'authentification de l'origine des données. <i>Note</i> – Tous les certificats sont réputés être des certificats de sécurité. Le terme <i>certificat de sécurité</i> est adopté dans la série UIT-T X.800 afin d'éviter des conflits de terminologie avec la Rec. UIT-T X.509.	X.810
domaine de sécurité (<i>security domain</i>)	1. Ensemble d'utilisateurs et de systèmes faisant l'objet de l'application d'une politique de sécurité commune. 2. Ensemble de ressources associé à une politique de sécurité unique.	X.841 X.411
information de sécurité (SI, <i>security information</i>)	Information nécessaire pour implémenter des services de sécurité.	X.810
gestion de la sécurité (<i>security management</i>)	La gestion de la sécurité englobe toutes les activités d'établissement, de maintien et de terminaison de caractéristiques de sécurité d'un système. Les sujets suivants sont traités: gestion de services de sécurité; installation de mécanismes de sécurité; gestion des clés (partie de gestion); établissement d'informations d'identité, de clés, de contrôle d'accès, etc.; gestion de la trace de l'audit de sécurité et des alarmes de sécurité.	M.3016.0
modèle de sécurité (<i>security model</i>)	Cadre pour décrire les services de sécurité destinés à faire face aux éventuelles menaces visant le système MTS et les éléments de sécurité qui sont à la base de ces services.	X.402
politique de sécurité (<i>security policy</i>)	1. Ensemble de règles fixées par l'autorité de sécurité qui régit l'utilisation et la fourniture de services et de fonctionnalités de sécurité. 2. Ensemble des critères permettant de fournir des services de sécurité. <i>Note</i> – Voir aussi politique de sécurité fondée sur l'identité (<i>identity-based security policy</i>) et politique de sécurité fondée sur des règles (<i>rule-based security policy</i>). Une politique de sécurité complète traite nécessairement de sujets qui ne relèvent pas du champ d'application de l'OSI.	X.509 X.800
service de sécurité (<i>security service</i>)	Service, fourni par une couche de systèmes ouverts, garantissant une sécurité des systèmes et du transfert de données.	X.800

Terme	Définition	Référence
menace de sécurité (menace) (<i>security threat (threat)</i>)	Violation potentielle de la sécurité	X.800
jeton de sécurité (<i>security token</i>)	Ensemble de données protégé par un ou plusieurs services de sécurité, ainsi que les informations de sécurité utilisées pour la fourniture de ces services de sécurité, qui est transféré entre les entités communicantes.	X.810
sensibilité (<i>sensitivity</i>)	Caractéristique d'une ressource liée à sa valeur ou à son importance.	X.509
secret partagé (<i>shared secret</i>)	Clé de sécurité pour les algorithmes cryptographiques; le secret partagé peut être déduit d'un mot de passe.	H.530
signature	Voir signature numérique (<i>digital signature</i>).	X.800
authentification simple (<i>simple authentication</i>)	Authentification utilisant de simples accords de mot de passe.	X.509
source d'autorité (SOA, <i>source of authority</i>)	Autorité d'attribut auquel peut faire confiance un vérificateur de privilège pour une ressource donnée, en tant qu'autorité ultime pour l'attribution d'un ensemble de privilèges.	X.509
spam	Courrier électronique non sollicité et non souhaité	H.235
usurpation d'identité (<i>spoofing</i>)	Usurpation de l'identité d'une ressource ou d'un utilisateur légitime	X.509
authentification forte (<i>strong authentication</i>)	Authentification utilisant des justificatifs obtenus par des moyens de chiffrement.	X.811
attaque Sybil	Attaque visant à corrompre le système de réputation d'un réseau entre homologues en créant un grand nombre d'entités pseudonymes et en les utilisant pour gagner une grande influence, totalement disproportionnée.	
menace (<i>threat</i>)	Violation potentielle de la sécurité.	X.800
jeton	Voir jeton de sécurité (<i>security token</i>)	
cheval de Troie (<i>Trojan horse</i>)	Un "cheval de Troie" est un programme introduit dans le système avec une fonction non autorisée, en plus de sa fonction autorisée. Un relais qui copie également des messages à destination d'une voie non autorisée est un "cheval de Troie".	X.800
confiance (<i>trust</i>)	On dit que l'entité X <i>fait confiance</i> à l'entité Y pour un ensemble d'activités si et seulement si l'entité X suppose que l'entité Y se comportera d'une certaine façon par rapport aux activités.	X.810
fonctionnalité de confiance (<i>trusted functionality</i>)	Fonctionnalité perçue comme correcte en ce qui concerne certains critères, tels que ceux qui sont définis par une politique de sécurité, par exemple.	X.800
tierce partie de confiance (TTP, <i>trusted third party</i>)	Autorité de sécurité ou son agent auquel d'autres entités font confiance au regard de certaines activités liées à la sécurité (dans le contexte d'une politique de sécurité).	X.810
réseau de capteurs ubiquitaires (USN, <i>ubiquitous sensor network</i>)	Réseau qui utilise des capteurs à faible coût et à faible puissance pour développer la perception du contexte afin de communiquer des données captées à toute personne, où qu'elle se trouve et à tout moment. Un réseau USN peut couvrir une grande zone géographique et peut prendre en charge diverses applications.	
accès non autorisé (<i>unauthorized access</i>)	Une entité tente d'accéder à des données en violation de la politique de sécurité en vigueur.	M.3016.0

Terme	Définition	Référence
authentification de l'utilisateur (<i>user authentication</i>)	Fourniture de la preuve de l'identité d'un utilisateur humain ou d'un processus d'application.	M.3016.0
vérificateur (<i>verifier</i>)	Entité qui est ou qui représente l'entité revendiquant une identité authentifiée. Un vérificateur comporte les fonctions nécessaires pour engager des échanges pour authentification.	X.811
vulnérabilité (<i>vulnerability</i>)	Toute faiblesse qui pourrait être exploitée pour violer un système ou les informations qu'il contient.	X.800
certificat UIT-T X.509 (<i>ITU-T X.509 certificate</i>)	Spécification de certificat de clé publique élaborée dans le cadre de la norme d'annuaire UIT-T X.500.	J.170

**Annexe B – Acronymes et abréviations utilisés
dans le présent manuel**

Annexe B

Acronymes et abréviations utilisés dans le présent manuel

Acronyme	Signification
ACI	information de contrôle d'accès (<i>access control information</i>)
AES	norme de chiffrement perfectionné (<i>advanced encryption standard algorithm</i>)
ASN.1	notation de syntaxe abstraite numéro un (<i>abstract syntax notation one</i>)
ASP	fournisseur de service d'application (<i>application service provider</i>)
ATIS	alliance for Telecommunications Industry Solutions
A/V	audiovisuel
BioAPI	interface de programmation d'application biométrique (<i>biometric application program/programming interface</i>)
BPON	réseau optique passif à large bande (<i>broadband passive optical network</i>)
B2C	entreprise-client (<i>business-to-customer</i>)
CA	autorité de certification (<i>certification authority</i>). Il s'agit d'une organisation de confiance qui accepte les demandes de certificat provenant des entités, authentifie les demandes, émet les certificats et tient à jour les informations d'état concernant les certificats.
CDMA	accès multiple par répartition en code (<i>code division multiple access</i>)
CMIP	protocole commun d'informations de gestion (<i>common management information protocol</i>)
CORBA	architecture de courtier commun de requêtes d'objets (<i>common object request broker architecture</i>)
CP	politique de certificat (<i>certificate policy</i>)
CPS	déclaration de pratique de certification (<i>certification practice statement</i>)
CRL	liste de révocation de certificats (<i>certificate revocation list</i>)
DNS	serveur/système/service de noms de domaine (<i>domain name server/system/service</i>)
DSL	boucle d'abonné numérique (<i>digital subscriber loop</i>)
EAP	protocole d'authentification extensible (<i>extensible authentication protocol</i>)
ENISA	Agence européenne chargée de la sécurité des réseaux et de l'information (<i>european network and information security agency</i>)
ETSI	Institut européen des normes de télécommunication (<i>european telecommunications standards institute</i>)
FMC	convergence fixe-mobile (<i>fixed mobile convergence</i>)
FW	pare-feu (<i>firewall</i>)
GK	portier (<i>gatekeeper</i>)
GPRS	système général de radiocommunications par paquets (<i>general packet radio system</i>)
GSM	système mondial de communications mobiles (<i>global system for mobile communications</i>)

Acronyme	Signification
GW	passerelle (<i>gateway</i>)
HFX	chiffrement de télécopie de Hawthorne (<i>Hawthorne facsimile cipher</i>)
HKM	algorithme de gestion de clés de Hawthorne (<i>Hawthorne key management algorithm</i>)
HTTP	protocole de transfert hypertexte (<i>hypertext transfer protocol</i>)
TIC	technologies de l'information et de la communication
ID	identificateur
IdM	gestion d'identité (<i>identity management</i>)
CEI	Commission électrotechnique internationale
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKE	L'échange de clés Internet (<i>Internet key exchange</i>) est un mécanisme de gestion de clés utilisé pour négocier et obtenir des clés pour des associations de sécurité (SA) dans le protocole IPSec.
IM	messagerie instantanée (<i>instant messaging</i>)
IMS	sous-système multimédia IP (<i>IP multimedia subsystem</i>)
IMT-2000	télécommunications mobiles internationales 2000 (<i>international mobile telecommunications 2000</i>)
IP	protocole Internet (<i>Internet protocol</i>)
IPSec	sécurité du protocole Internet (<i>Internet protocol security</i>)
TVIP	télévision utilisant le protocole Internet
IPX	échange de paquets Internet (<i>Internet packet exchange</i>)
ISMS	système de gestion de la sécurité des informations (<i>information security management system</i>)
ISO	Organisation internationale de normalisation (<i>international organization for standardization</i>)
UIT-T	Secteur de la normalisation des télécommunications de l'Union internationale des télécommunications
LAN	réseau local (<i>local area network</i>)
LDAP	protocole rapide d'accès à l'annuaire (<i>lightweight directory access protocol</i>)
MD5	condensé de message N° 5 (<i>message digest No. 5</i>) (algorithme de hachage sécurisé)
MIS	système d'informations de gestion (<i>management information system</i>)
MTA	agent de transfert de messages (<i>message transfer agent</i>) (dans les systèmes de messagerie) adaptateur de terminal média (<i>media terminal adapter</i>) (dans les systèmes de transmission par câble)
MWSSG	passerelle de sécurité pour les services web mobiles (<i>mobile web services security gateway</i>)
NAT	traduction d'adresse réseau (<i>network address translation</i>)
NGN	réseau de prochaine génération (<i>next generation network</i>)
OASIS	Organization for the Advancement of Structured Information Standards
OMG	Object Management Group

Acronyme	Signification
OSI	interconnexion des systèmes ouverts (<i>open systems interconnection</i>)
P2P	homologue à homologue (<i>peer-to-peer</i>)
PC	ordinateur personnel (<i>personal computer</i>)
PDA	assistant personnel électronique (<i>personal data assistant</i>)
PIN	numéro d'identification personnel (<i>personal identification number</i>)
PII	information d'identification personnelle (<i>personally identifiable information</i>)
PKI	infrastructure de clé publique (<i>public-key infrastructure</i>)
PKINIT	authentification initiale par cryptographie à clé publique (<i>public-key cryptography initial authentication</i>)
PMI	infrastructure de gestion de privilège (<i>privilege management infrastructure</i>)
PSS	service de protection des informations PII (<i>PII protection service</i>)
RTPC	réseau téléphonique public commuté
QoS	qualité de service (<i>quality of service</i>)
RBAC	contrôle d'accès basé sur le rôle (<i>role-based access control</i>)
RFID	identification par radiofréquence (<i>radio frequency identification</i>)
RSA	Rivest, Shamir et Adleman (algorithme à clé publique)
RTP	protocole de transport en temps réel (<i>real time protocol</i>)
SAML	langage de balisage d'assertion de sécurité (<i>security assertion markup language</i>)
CE	Commission d'études
SHA1	algorithme de hachage sécurisé numéro un (<i>secure hash algorithm 1</i>)
SIP	protocole d'ouverture de session (<i>session initiation protocol</i>). Protocole (de signalisation) de commande de la couche application permettant de créer, de modifier et de terminer des sessions avec un ou plusieurs participants.
SMS	service de messages courts (<i>short message service</i>)
SMTP	protocole simple de transfert de courrier (<i>simple mail transfer protocol</i>)
SNMP	protocole simple de gestion de réseau (<i>simple network management protocol</i>)
SoA	source d'autorité (<i>source of authority</i>)
SOA	architecture orientée service (<i>service oriented architecture</i>)
SPAK	protocole d'authentification sûre fondée sur un mot de passe avec échange de clés (<i>secure password-based authentication protocol with key exchange</i>)
SSL	couche de connecteurs sécurisés (<i>secure socket layer</i>)
SSO	connexion unique (<i>single sign-on</i>)
TCP/IP	Protocole de commande de transmission/protocole Internet (<i>transmission control protocol/internet protocol</i>)
TLS	sécurité de la couche transport (<i>transport layer security</i>)
RGT	réseau de gestion des télécommunications

Acronyme	Signification
UE	équipement d'utilisateur (<i>user equipment</i>)
UICC	carte de circuit intégré universelle (<i>universal integrated circuit card</i>)
USN	réseau de capteurs ubiquitaires (<i>ubiquitous sensor network</i>)
VoIP	téléphonie IP, voix sur IP (<i>voice over IP</i>)
VPN	réseau privé virtuel (<i>virtual private network</i>)
WAN	réseau étendu (<i>wide area network</i>)
Wi-Fi	fidélité sans fil (<i>wireless fidelity</i>) (marque déposée de l'Alliance Wi-Fi pour les produits certifiés basés sur les normes IEEE 802.11)
AMNT	Assemblée mondiale de normalisation des télécommunications
XACML	langage de balisage extensible de contrôle d'accès (<i>extensible access control markup language</i>)
XML	langage de balisage extensible (<i>extensible markup language</i>)
3G	troisième génération (<i>3rd generation</i>)
3GPP	projet de partenariat de troisième génération (<i>3rd generation partnership project</i>)
3GPP2	projet de partenariat de troisième génération numéro deux (<i>3rd generation partnership project 2</i>)

**Annexe C – Présentation succincte des
Commissions d'études de l'UIT-T menant
des activités dans le domaine de la sécurité**

Annexe C

Présentation succincte des Commissions d'études de l'UIT-T menant des activités dans le domaine de la sécurité

La plupart des Commissions d'études étudient au moins certains aspects de la sécurité des télécommunications et/ou des TIC. La Commission d'études 17, dont le domaine d'étude général est la sécurité, a été désignée Commission d'études directrice pour la sécurité et chacune des autres Commissions d'études est chargée d'étudier les questions de sécurité qui relèvent de son propre domaine de compétence. Le Tableau 8 répertorie les Commissions d'études ayant des responsabilités dans le domaine de la sécurité et énumère les rôles qu'elles ont en tant que Commission d'études directrice.

Tableau 8 – Commissions d'études ayant des responsabilités dans le domaine de la sécurité

Commission d'études	Titre	Responsabilités/rôle dans le domaine de la sécurité
CE 2	Aspects opérationnels de la fourniture de services et de la gestion des télécommunications	Commission d'études directrice pour la définition des services, le numérotage et le routage Commission d'études directrice pour les télécommunications utilisées pour les secours en cas de catastrophe/l'alerte avancée Commission d'études directrice pour la gestion des télécommunications
CE 5	Environnement et changement climatique	Commission d'études directrice pour la compatibilité électromagnétique et les effets électromagnétiques Commission d'études directrice pour les TIC et le changement climatique
CE 9	Transmission télévisuelle et sonore et réseaux câblés intégrés à large bande	Commission d'études directrice pour les réseaux de télévision et câblés intégrés large bande
CE 11	Spécifications de signalisation, protocoles et spécifications de test	Commission d'études directrice pour la signalisation et les protocoles Commission d'études directrice pour les réseaux intelligents Commission d'études directrice pour les spécifications de test
CE 12	Qualité de fonctionnement, qualité de service et qualité d'expérience	Commission d'études directrice pour la qualité de service et la qualité d'expérience
CE 13	Réseaux futurs, y compris les réseaux mobiles et les réseaux de prochaine génération	Commission d'études directrice pour les réseaux futurs et les NGN Commission d'études directrice pour la gestion de la mobilité et la convergence fixe-mobile
CE 15	Infrastructures des réseaux de transport optiques et des réseaux d'accès	Commission d'études directrice pour le transport dans le réseau d'accès Commission d'études directrice pour les technologies optiques Commission d'études directrice pour les réseaux de transport optiques

CE 16	Codage, systèmes et applications multimédias	Commission d'études directrice pour le codage, les systèmes et les applications multimédias Commission d'études directrice pour les applications ubiquitaires ("tout en ligne", par exemple la cybersanté) Commission d'études directrice pour l'accessibilité des télécommunications/TIC pour les personnes handicapées
CE 17	Sécurité	Commission d'études directrice pour la sécurité des télécommunications Commission d'études directrice pour la gestion d'identité Commission d'études directrice pour les langages et les techniques de description

Annexe D – Recommandations sur la sécurité mentionnées dans le présent manuel

Annexe D

Recommandations sur la sécurité mentionnées dans le présent manuel

La présente annexe contient une liste complète de toutes les Recommandations UIT-T mentionnées dans le présent manuel avec des hyperliens, ce qui permet, à partir de la version électronique du texte, d'accéder directement aux Recommandations et de les télécharger. Comme indiqué dans le texte, l'UIT-T a élaboré de nombreuses normes relatives à la sécurité en collaboration avec d'autres organisations de normalisation. Les Recommandations en vigueur relatives à la sécurité des TIC dont le texte a été établi en commun avec une autre organisation sont également incluses dans ce tableau. L'ensemble complet des Recommandations UIT-T est accessible en ligne à l'adresse suivante: www.itu.int/rec/T-REC/en. Les Recommandations UIT-T relatives à la sécurité sont disponibles via la Partie 2 (base de données) de la feuille de route sur les normes de sécurité (www.itu.int/ITU-T/studygroups/com17/ict/index.html).

Recommandation	Titre	Texte équivalent
E.408	Prescriptions de sécurité des réseaux de télécommunication	
E.409	Organisation en cas d'incident et prise en charge des incidents relatifs à la sécurité: lignes directrices destinées aux organisations de télécommunication	
G.827	Paramètres et objectifs de disponibilité pour les conduits numériques internationaux de bout en bout à débit constant	
G.1000	Qualité de service des communications: cadre et définitions	
G.1030	Evaluation de la qualité de fonctionnement de bout en bout dans les réseaux IP pour les applications de transmission de données	
G.1050	Modèle de réseau pour l'évaluation de la qualité de transmission multimédia sur protocole Internet	
G.1081	Points de surveillance de la qualité de fonctionnement pour la TVIP	
H.235.0	Cadre de sécurité H.323: cadre de sécurité pour les systèmes multimédias de la série H (systèmes H.323 et autres systèmes de type H.245)	
H.235.1	Cadre de sécurité H.323: profil de sécurité de base	
H.235.2	Cadre de sécurité H.323: profil de sécurité avec signature	
H.235.3	Cadre de sécurité H.323: profil de sécurité hybride	
H.235.4	Cadre de sécurité H.323: sécurité des appels à routage direct et des appels à routage sélectif	
H.235.5	Cadre de sécurité H.323: cadre de l'authentification sécurisée pendant l'échange de messages RAS au moyen de secrets partagés faibles	
H.235.6	Cadre de sécurité H.323: profil pour le chiffrement vocal avec gestion de clés native dans les systèmes H.235/H.245	
H.Imp235	Implementors Guide for H.235 V3: "Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals"	
H.323	Systèmes de communication multimédia en mode paquet	
H.350	Architecture des services d'annuaire pour les conférences multimédias	
H.460.17	Utilisation de la connexion de signalisation d'appel H.225.0 pour le transport de messages RAS H.323	

Recommandation	Titre	Texte équivalent
H.460.18	Traversée de traducteurs d'adresse de réseau et de pare-feu par des flux de signalisation H.323	
H.460.19	Traversée de traducteurs d'adresse de réseau et de pare-feu par des flux de média H.323	
H.510	Mobilité pour systèmes et services multimédias H.323	
H.530	Procédures de sécurité symétrique pour la mobilité des systèmes H.323 selon la Recommandation H.510	
J.160	Cadre architectural pour l'acheminement de services à temps critique sur les réseaux de télévision par câble utilisant des câblo-modems	
J.170	Spécification de la sécurité sur IPCablecom	
J.360	Architecture générale IPCablecom2	
M.3010	Principes du réseau de gestion des télécommunications	
M.3016.0	Sécurité pour le plan de gestion: aperçu général	
M.3016.1	Sécurité pour le plan de gestion: prescriptions de sécurité	
M.3016.2	Sécurité pour le plan de gestion: services de sécurité	
M.3016.3	Sécurité pour le plan de gestion: mécanisme de sécurité	
M.3016.4	Sécurité pour le plan de gestion: Formulaire des profils de sécurité	
M.3208.2	Services de gestion RGT pour réseaux à circuits spécialisés et circuits reconfigurables: gestion des connexions de liaison de service préapprouvées pour la formation d'un service de circuit loué	
M.3210.1	Services de gestion RGT pour la gestion de la sécurité des réseaux IMT-2000	
Q.816	Services RGT à architecture CORBA	
Q.834.3	Description en langage UML des prescriptions relatives aux interfaces de gestion des réseaux optiques passifs à large bande	
Q.834.4	Spécification d'une interface en architecture CORBA pour les réseaux optiques passifs à large bande basée sur les prescriptions d'interface UML	
Q.1701	Cadre général des réseaux IMT-2000	
Q.1702	Aspects réseau au-delà des systèmes IMT-2000 – Vision à long terme	
Q.1703	Cadre général des capacités de service et de réseau des aspects réseau des systèmes au-delà de l'IMT-2000	
Q.1741.1	Références IMT-2000 à la version 1999 du réseau central UMTS issu du GSM avec réseau d'accès radioélectrique universel de Terre (UTRAN)	3GPP
Q.1742.1	Références IMT-2000 au réseau central évolué ANSI-41 avec réseau d'accès cdma2000	3GPP2
T.4	Normalisation des télécopieurs du Groupe 3 pour la transmission de documents	
T.36	Capacités de sécurité à utiliser avec les télécopieurs du Groupe 3	
T.37	Procédures pour le transfert de données de télécopie en mode différé sur le réseau Internet	
T.38	Procédures de communication de télécopie du Groupe 3 en temps réel sur les réseaux à protocole Internet	
T.563	Caractéristiques des télécopieurs du groupe 4	
X.500	L'annuaire: aperçu général des concepts, modèles et services	ISO/CEI 9594-1
X.501	L'annuaire: les modèles	ISO/CEI 9594-2
X.509	L'annuaire: cadre général des certificats de clé publique et d'attribut	ISO/CEI 9594-8

Recommandation	Titre	Texte équivalent
X.511	L'annuaire: définition du service abstrait	ISO/CEI 9594-3
X.518	L'annuaire: procédures pour le fonctionnement réparti	ISO/CEI 9594-4
X.519	L'annuaire: spécification des protocoles	ISO/CEI 9594-5
X.520	L'annuaire: types d'attributs sélectionnés	ISO/CEI 9594-6
X.521	L'annuaire: classes d'objets sélectionnées	ISO/CEI 9594-7
X.525	L'annuaire: duplication	ISO/CEI 9594-9
X.530	L'annuaire: utilisation de la gestion-systèmes pour l'administration de l'annuaire	ISO/CEI 9594-10
X.711	Protocole commun d'information de gestion: spécification	ISO/CEI 9596-1
X.736	Gestion-systèmes: fonction de signalisation des alarmes de sécurité	ISO/CEI 10164-7
X.740	Gestion-systèmes: fonction de piste de vérification de sécurité	ISO/CEI 10164-8
X.741	Gestion-systèmes: objets et attributs de contrôle d'accès	ISO/CEI 10164-9
X.780	Directives concernant le RGT pour la définition d'objets gérés CORBA	
X.780.1	Directives concernant le RGT pour la définition d'interfaces d'objets gérés CORBA à granularité grossière	
X.780.2	Lignes directrices relatives au RGT pour la définition d'objets gérés et d'objets de façade CORBA orientés service	
X.781	Spécifications et directives pour l'établissement de formulaires de déclaration de conformité d'implémentations associés aux systèmes de type CORBA	
X.790	Fonction de gestion des dérangements pour les applications de l'UIT-T	
X.800	Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT	ISO/CEI 7498-2
X.802	Modèle de sécurité des couches inférieures	ISO/CEI TR 13594
X.803	Modèle de sécurité pour les couches supérieures	ISO/CEI 10745
X.805	Architecture de sécurité pour les systèmes assurant des communications de bout en bout	ISO/CEI 18028-2
X.810	Cadres de sécurité pour les systèmes ouverts: aperçu général	ISO/CEI 10181-1
X.811	Cadres de sécurité pour les systèmes ouverts: cadre d'authentification	ISO/CEI 10181-2
X.812	Cadres de sécurité pour les systèmes ouverts: cadre de contrôle d'accès	ISO/CEI 10181-3
X.813	Cadres de sécurité pour les systèmes ouverts: non-répudiation	ISO/CEI 10181-4
X.814	Cadres de sécurité pour les systèmes ouverts: cadre de confidentialité	ISO/CEI 10181-5
X.815	Cadres de sécurité pour les systèmes ouverts: cadre d'intégrité	ISO/CEI 10181-6
X.816	Cadres de sécurité pour les systèmes ouverts: cadre d'audit et d'alarmes de sécurité	ISO/CEI 10181-7
X.830	Sécurité générique des couches supérieures: aperçu général, modèles et notation	ISO/CEI 11586-1
X.831	Sécurité générique des couches supérieures: définition du service assuré par l'élément de service d'échange de sécurité	ISO/CEI 11586-2
X.832	Sécurité générique des couches supérieures: spécification du protocole d'élément de service d'échange de sécurité	ISO/CEI 11586-3
X.833	Sécurité générique des couches supérieures: spécification de la syntaxe de protection du transfert	ISO/CEI 11586-4

Recommandation	Titre	Texte équivalent
X.834	Sécurité générique des couches supérieures: formulaire PICS de l'élément de service d'échange de sécurité (SESE)	ISO/CEI 11586-5
X.835	Sécurité générique des couches supérieures: formulaire PICS de la syntaxe de protection de transfert	ISO/CEI 11586-6
X.841	Techniques de sécurité – Objets informationnels de sécurité pour le contrôle d'accès	ISO/CEI 15816
X.842	Techniques de sécurité – Lignes directrices pour l'utilisation et la gestion des services de tiers de confiance	ISO/CEI TR 14516
X.843	Techniques de sécurité – Spécification de services de tiers de confiance pour la prise en charge des applications de signature numérique	ISO/CEI 15945
X.Sup3 à X.800- X.849	Lignes directrices pour la mise en œuvre de la sécurité dans les systèmes et dans les réseaux	
X.1031	Rôle des utilisateurs finals et des réseaux de télécommunication dans l'architecture de sécurité	
X.1034	Lignes directrices sur l'authentification et la gestion de clé basées sur le protocole d'authentification extensible dans un réseau de communication de données	
X.1035	Protocole d'échange de clés avec authentification par mot de passe	
X.1036	Cadre applicable à la création, au stockage, à la distribution et à la mise en vigueur des politiques de sécurité de réseau	
X.1051	Techniques de sécurité – Lignes directrices basées sur la norme ISO/CEI 27002 pour la gestion de la sécurité des informations pour les organisations de télécommunication	ISO/CEI 27011
X.1055	Guide concernant la gestion des risques et les profils de risques	
X.1056	Lignes directrices relatives à la gestion des incidents de sécurité dans les télécommunications	
X.1081	Cadre général pour la spécification des aspects de sécurité et d'innocuité de la télébiométrie	
X.1082	Télébiométrie relative à la physiologie humaine	ISO/CEI 80000-14
X.1083	Biométrie – Protocole d'interfonctionnement à l'interface BioAPI	ISO/CEI 24708
X.1084	Mécanisme de système télébiométrique – Partie 1: Protocole général d'authentification biométrique et profils types pour les systèmes de télécommunication	
X.1086	Procédures de protection télébiométriques – Partie 1: Lignes directrices relatives aux mesures techniques et de gestion pour la sécurité des données biométriques	
X.1088	Cadre général des clés numériques télébiométriques – Cadre pour la génération et la protection des clés numériques biométriques	
X.1089	Infrastructure d'authentification télébiométrique	
X.1111	Cadre général des technologies de sécurité pour les réseaux domestiques	
X.1112	Profil de certificat pour les dispositifs présents dans le réseau domestique	
X.1113	Lignes directrices applicables aux mécanismes d'authentification de l'utilisateur pour les services assurés dans le réseau domestique	
X.1114	Cadre d'autorisation pour le réseau domestique	
X.1121	Cadre général des technologies de la sécurité pour les communications mobiles de données de bout en bout	

Recommandation	Titre	Texte équivalent
X.1122	Lignes directrices pour la réalisation de systèmes mobiles sécurisés basés sur l'infrastructure de clés publiques (PKI)	
X.1123	Service de sécurité différencié pour les communications mobiles sécurisées de bout en bout	
X.1124	Architecture d'authentification pour les communications de données de bout en bout dans les réseaux mobiles	
X.1125	Système de réaction corrélative pour les communications de données dans les réseaux mobiles	
X.1141	Langage de balisage d'assertion de sécurité (SAML 2.0)	OASIS SAML 2.0
X.1142	Langage de balisage extensible de contrôle d'accès (XACML 2.0)	OASIS XACML 2.0
X.1143	Architecture de sécurité des messages dans l'environnement des services web mobiles	
X.1151	Lignes directrices applicables à un protocole d'authentification sûre fondée sur un mot de passe avec échange de clés	
X.1152	Techniques de communication de données de bout en bout sécurisée reposant sur des services de tiers de confiance	
X.1161	Cadre général des communications sécurisées entre homologues	
X.1162	Architecture de sécurité et opérations dans les réseaux entre homologues	
X.1171	Menaces et protection requise pour les informations d'identification personnelle dans les applications utilisant l'identification par étiquette	
X.1191	Spécifications fonctionnelles et architecture concernant les aspects de sécurité de la TVIP	
X.1205	Présentation générale de la cybersécurité	
X.1206	Cadre indépendant du fournisseur de produits pour la notification automatique d'informations de sécurité et la diffusion automatique de mises à jour	
X.1207	Lignes directrices à l'intention des fournisseurs de services de télécommunication pour lutter contre les risques d'installation de logiciels espions ou de tout logiciel potentiellement indésirable	
X.1231	Stratégies techniques de lutte contre le spam	
X.1240	Technologies intervenant dans la lutte contre le spam par courrier électronique	
X.1241	Cadre technique pour lutter contre les spams par courrier électronique	
X.1242	Système de filtrage des spams du service de messages courts (SMS) basé sur des règles spécifiées par l'utilisateur	
X.1244	Aspects généraux de la lutte contre le spam dans les applications multimédias IP	
X.1250	Capacités de base pour l'amélioration de la confiance et de l'interopérabilité globales dans la gestion d'identité	
X.1251	Cadre de contrôle de l'identité numérique par l'utilisateur	
X.1303	Protocole d'alerte commun (CAP 1.1)	OASIS CAP v1.1
X.Sup6	Série UIT-T X.1240 – Supplément sur la lutte contre le spam et les menaces associées	
X.Sup7	Série UIT-T X.1250 – Supplément sur un aperçu de la gestion d'identité dans le contexte de la cybersécurité	
Y.2001	Aperçu général des réseaux de prochaine génération	

Recommandation	Titre	Texte équivalent
Y.2701	Prescriptions de sécurité des réseaux de prochaine génération de version 1	
Y.2720	Cadre de gestion d'identité dans les NGN	
	Autres publications	
	Technologies des installations extérieures appliquées aux réseaux publics	
	Application des ordinateurs et des microprocesseurs à la fabrication, à l'installation et à la protection des câbles de télécommunication	

